Comisión de Regulación de Comunicaciones
REPÚBLICA DE COLOMBIA

# Identificación de las posibles acciones regulatorias a implementar en materia de Ciberseguridad

Documento de análisis y consulta

**Coordinación Relaciones de Gobierno y Asesoría**

Julio de 2015

# CONTENIDO

# 1. INTRODUCCIÓN

En la actualidad la seguridad personal, empresarial y nacional en el ciberespacio, son temas de importancia vital y estratégica a nivel mundial. Es así como de acuerdo con Wegener (2014) "*Todos sabemos que los retos de la sociedad de la información solo se pueden superar a través de una estrecha cooperación internacional y de una posible normativa y regulación universal. La política de ciberseguridad global significa la colaboración de los países, pero también la de todos los actores digitales. El planteamiento de la comunidad Multi-Stakeholder está en boca de todos, y lo está porque es irrenunciable. El concepto tradicional de soberanía resulta insuficiente en la lucha contra el ciberconflicto. Ningún estado, ningún grupo de estados y ninguna organización internacional son autónomos respecto a la situación que caracteriza a una exigente política de ciberseguridad global y los campos de acción regionales son incluso tan esenciales como los estados individuales.*"[1]

Dada esta importante necesidad, la Comisión de Regulación Comunicaciones – CRC-, en su Agenda Regulatoria 2014-2015 incluyó el proyecto *"Condiciones regulatorias en materia de Ciberseguridad[2]"*, dentro del cual se adelantó un análisis para identificar el rol que tiene la CRC en el desarrollo de estos temas y en la definición de medidas regulatorias que contribuyan a preservar la seguridad de las redes y servicios dentro de un enfoque orientado a contrarrestar el incremento de las amenazas informáticas que afectan a los usuarios de servicios de comunicaciones, y potencialmente al país, así como identificar posibles recomendaciones para otras entidades involucradas en la Estrategia Nacional de Ciberseguridad y Ciberdefensa.

Por lo tanto, el presente documento presenta el análisis de la información vigente en temas de Ciberseguridad, a nivel nacional e internacional, incluyendo la información y documentación suministrada por el Ministerio de Tecnologías de la Información y las Comunicaciones, la revisión de las recomendaciones hechas por la UIT-T, OECD, y el documento elaborado por la OEA como *Misión de Asistencia Técnica en Seguridad Cibernética* para Colombia[3]; todo esto con el fin de plantear posibles líneas de acción en la materia para la Comisión de Regulación de Comunicaciones, así como apoyar la actualización y consolidación de la Estrategia Nacional de Ciberseguridad y Ciberdefensa

[1] Wegener, Henning. La Ciberseguridad en la Unión Europea. Instituto español de estudios estratégicos. http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO77bis-2014_CiberseguridadProteccionInformacion_H.Wegener.pdf

[2] La Ciberseguridad se define como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos y organizaciones tanto públicas como privadas, ante amenazas o incidentes de naturaleza cibernética (Documento CONPES 3701 de 2011).

[3] Publicado en http://www.oas.org/documents/spa/press/Recomendaciones_COLOMBIA_SPA.pdf

para los próximos años, actuando de una forma coordinada con las entidades involucradas en dicha estrategia.

En este sentido, al final del presente documento se incluye una Consulta Pública encaminada a conocer las opiniones y sugerencias de los agentes del sector involucrados en la materia, en cuanto a cómo se percibe la participación de la CRC desde el ámbito de sus competencias en temas regulatorios que estén relacionados con Ciberseguridad y Ciberdefensa, así como su participación junto a otras Entidades en la actualización y fortalecimiento de la Estrategia Nacional de Ciberseguridad y Ciberdefensa.

## 2. ANTECEDENTES

La CRC mediante la Resolución CRC 2258 de 2009[4] estableció las medidas que deben implementar los PRST en sus redes con el objetivo de garantizar la seguridad en las mismas, sin embargo esta resolución fue derogada por la Resolución CRC 3066 de 2011 la cual consagra el *"Régimen integral de protección de los derechos de los usuarios de los servicios de comunicaciones"*, en este régimen se establecieron las disposiciones aplicables a su red en materia de seguridad para que contribuyan a mejorar la seguridad de sus redes de acceso, de acuerdo con la Recomendación UIT-T X.805, así mismo cumplir con los establecido mediante la Resolución CRC 3067 de 2011 en cuanto a principios de confidencialidad, protección de los datos personales, inviolabilidad de las comunicaciones, seguridad de la información y prevención de fraudes

Posteriormente, tras la aprobación del CONPES 3701 de 2011 se definió en Colombia la estrategia del Gobierno Nacional y la Fuerza Pública, en materia de Ciberseguridad y Ciberdefensa[5], siendo uno de los primeros países de América Latina, en adoptar una estrategia para prevenir y enfrentar delitos informáticos y minimizar el nivel de riesgo de ciudadanos ante amenazas o incidentes de naturaleza cibernética.

---

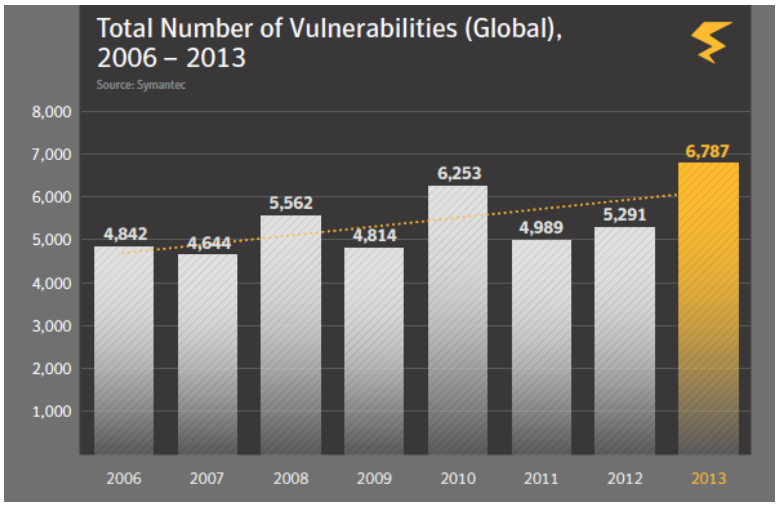
[4] Dicha resolución establecía la obligación, para los proveedores de redes y/o servicios de telecomunicaciones que ofrezcan acceso a Internet, de implementar modelos de seguridad, de acuerdo con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso, de acuerdo con los marcos de seguridad definidos por la UIT-T X-805, 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. Asimismo, estableció 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 los datos e informaciones.

[5] Ciberdefensa se define como la capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional, (Documento CONPES 3701 de 2011).

A nivel de contexto es importante tener en cuenta que debido al gran despliegue tecnológico en las redes de comunicaciones, de banda ancha e implementación de la tecnología 4G en el país; es evidente el aumento en el uso de las tecnologías de la información, en actividades tales como: el comercio electrónico, la banca móvil, el uso de redes sociales, las descargas multimedia *Over-the-top,* y en general para muchas otras actividades de la vida cotidiana de los usuarios; con lo cual se presentan nuevos retos, riesgos y amenazas vinculadas al uso de la tecnología, lo cual requiere un constante seguimiento y propuestas que contribuyan a la protección de los usuarios de los servicios de comunicaciones.

De acuerdo con un estudio realizado por Symantec en 2014 para la OEA[6], los usuarios de Latinoamérica y el Caribe se ven afectados por amenazas que también son reportadas a nivel global. Por ejemplo se presentaron 6787 vulnerabilidades reportadas en portales web en 2013 lo cual muestra una tendencia creciente la gran mayoría de años.

**Gráfico No. 1** Evolución de vulnerabilidades en redes




Fuente: Symantec

El año 2013 fue denominado *"El año de las grandes violaciones de la seguridad cibernética"* debido al significativo aumento en las violaciones a los datos, es así como más de 552 millones de identidades quedaron expuestas a causa de estas violaciones a los datos, lo que puso en riesgo información relacionada con tarjetas de crédito, datos financieros, médicos y otros tipos de información personal

[6] http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

de los consumidores mediante delitos cibernéticos y actos de Hacktivismo[7]; de igual forma en el 2014 se presentaron diferentes ataques de gran repercusión en el que se destaca el ataque a la red Sony Entertainment, haciendo que la empresa perdiera información importante de los usuarios conectados a través de las consolas de videojuegos Playstation, ingresaron en la bases de datos de la empresa y extrajeron proyectos fílmicos que en su momento no habían dado a conocerse. Ahora bien, si buscamos en internet ataques cibernéticos y delitos informáticos es fácil encontrar todo tipo de hacking y objetos maliciosos distribuidos a través de la red como se ha comentado en varios escenarios, alrededor de 3 nuevos virus son creados cada segundo en el mundo[8], es evidente el crecimiento de ataques dirigidos contra personas u organizaciones usuarios de internet, hoy en día los delincuentes cibernéticos adaptan las campañas de *spear-phishing* (robo de identidad con objetivos específicos) y ataques denominados *watering-hole* (que se valen de las visitas a una página web), las estafas en redes sociales crecen cada día y delincuentes cibernéticos expresan su particular interés en obtener los datos que compartimos en Internet.

En el mismo estudio de Symantec, en toda América Latina y el Caribe, la cantidad de incidentes que involucran troyanos bancarios aumentó considerablemente, ataques como el malware dirigido a cajeros automáticos se descubrió por primera vez en México y se ha extendido a otros países de América, especialmente en países hispanohablantes. Eventos de gran convocatoria siempre son atractivos para los delincuentes, como lo fue la Copa del Mundo de la FIFA 2014 en la cual los delincuentes cibernéticos realizaron incontables operaciones de malware, *phishing* y estafas por correo electrónico relacionadas al tema del evento. De otro lado, en países como Guatemala, Paraguay, y Venezuela se ha presentado un incremento hasta en un 40% de los ataques de denegación de servicios (DoS y DDoS), en especial a páginas web del Estado.

En Colombia, de acuerdo con estadísticas del Centro Cibernético de la Policía Nacional –CCP- para Colombia, se han identificado 3 tendencias específicas de cibercrimen:

[7] http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf The term "Hacktivism" combines the words hack and activism. It describes hacking activities performed to promote a political ideology. For more information, see: Anderson , Hacktivism and Politically Motivated Computer Crime, 2005, available at: http://www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf.
[8] http://www.adnmundo.com/contenidos/73000_virus_informaticos_malewares_por_dia_te_2332011.html

**Gráfico No. 2.** Tendencias de cibercrimen

**Uso de código malicioso, phishing y robo de información**

- Afectan principalmente a usuarios e instituciones que operan en el creciente sector de la banca virtual, y el problema radica básicamente en una situación particular de una débil cultura de la seguridad y una correspondiente falta de concientización de los usuarios.

**Autorización de acceso a información o fuga, interceptación de datos, acceso abusivo a los sistemas, denegación del servicio (DoS), vandalismo en sitio Web**

- Principalmente impactan y están enmarcadas en generar incidentes que afecten la seguridad cibernética y pongan en apuros a organizaciones y entidades del estado, o compañías.

**Uso de redes sociales, correo electrónico y la Internet profunda por delincuentes comunes y el crimen organizado.**

- Comprende el cobro masivo ilegal de dinero (por ejemplo, pirámides cibernéticas), el uso de divisas virtuales como mecanismo para lavar dinero y negocios ilícitos que involucran el tráfico de armas, las drogas, la pornografía infantil, etcétera

Fuente: CRC con información de Centro Cibernético de la Policía Nacional para Colombia

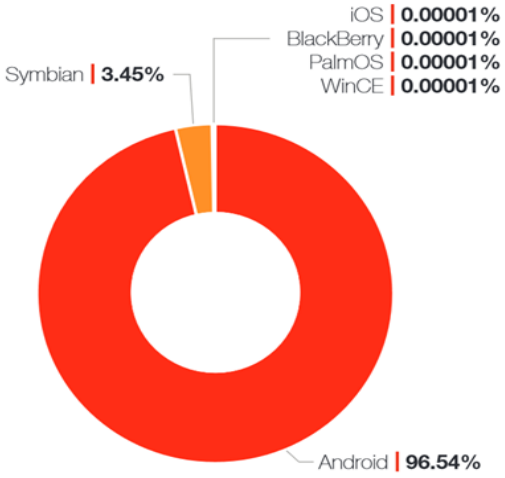
Del año 2014, se tiene reporte por parte del Centro Cibernético de la Policía Nacional para Colombia, que 13.604 páginas web fueron bloqueadas por pornografía infantil disminuyendo un 8,09% con respecto al año 2013; de igual manera se presentaron 6.351 nuevas alertas de amenazas cibernéticas evidenciando un incremento de 23,94%, de los 8.996 ataques o incidentes cibernéticos reportados el 87.36% involucró a ciudadanos particulares, y el 7.86% a entidades del sector bancario, el resto de los incidentes involucró a una combinación casi igual de entidades pertenecientes a los sectores de gobierno, fuerzas de seguridad, comunicaciones, energía, salud y educación.

De manera particular, es importante tener en cuenta las amenazas crecientes en términos de seguridad informática, en los dispositivos móviles debido a los cambios en las tendencias de uso de Internet por parte de los usuarios, quienes han pasado de los computadores de escritorio a los portátiles, y de ahí a los dispositivos móviles, especialmente aquellos que utilizan plataformas de código abierto, debido a que usan interfaces simples y tienen alta popularidad. Esta situación se evidencia en el gran crecimiento, en los últimos años, en el desarrollo de malware para estos dispositivos.

De acuerdo con Fortiguard, empresa que ha recolectado muestras de malware desde 2011 hasta 2014, los dispositivos móviles perdidos o robados suelen aumentar actividades móviles maliciosas, aunque el comportamiento imprudente de los usuarios de teléfonos celulares los vuelve susceptibles a

muchos tipos de ataques posibles. Los usuarios de teléfonos celulares demuestran un comportamiento imprudente cuando almacenan archivos sensibles de la siguiente manera; online (52%), guardan información laboral y personal en las mismas cuentas de almacenamiento online (24%) y comparten contraseñas y claves de acceso con familiares (21%) y amigos (18%), lo cual pone en riesgo todos sus datos e información. Únicamente 50% de esos usuarios toma las precauciones de seguridad más básicas, mientras que el resto descarta el uso de contraseñas o programas de seguridad en sus dispositivos móviles, se observa un crecimiento exponencial, especialmente en los últimos dos años en malware en móviles[9].

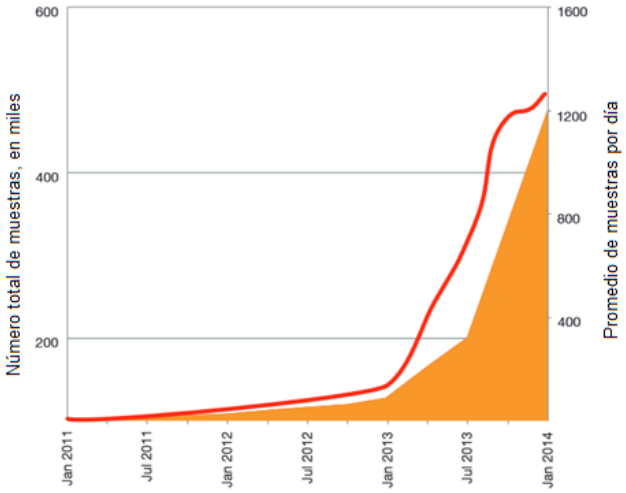
**Gráfico No. 3.** Porcentaje de participación en malware por Sistema Operativo




Fuente: Fortiguard

[9] https://www.clickssl.com/blog/android-becomes-the-dominant-player-in-spreading-mobile-malware

**Gráfico No. 4**. Número de muestras de malware en Android.




Fuente: Fortiguard.

En materia de los servicios prestados de Computación en la Nube o Cloud Computing, existen documentos de estudio a nivel internacional[10] que han evaluado estos temas y a su vez han desarrollado algunos análisis; las recomendaciones están enmarcadas fundamentalmente en los siguientes aspectos:

- **Contexto de la negociación**: En donde se especifiquen de manera clara y concisa los servicios que se van a prestar, además de los elementos críticos de dichos servicios y la procedencia del proveedor.
- **La seguridad ofrecida**: Estableciendo claramente la responsabilidad por acceso o pérdida, los procedimientos para toma de evidencia digital, las obligaciones regulatorias aplicables para cada sector en materia de protección de datos personales, las cláusulas de confidencialidad, protocolos de seguridad y auditorías, obligaciones de retención de la información y notificaciones de violación de seguridad.
- **La ubicación de la información**: Determinando la normatividad aplicable en materia de protección de datos y evidencias digitales.
- **Los Acuerdos de Niveles de Servicio (Service Level Agreement - SLA)**: En donde se determine cuándo un incumplimiento en un nivel de servicio se constituye en un

[10] García del Pollo, Rafael. *"Cloud Computing: Aspectos jurídicos clave para la contratación de estos servicios" . Disponible en* http://tinyurl.com/pd92qn8.

incumplimiento contractual, créditos, multas y limitación de responsabilidades, además de mecanismos de revisión y mejora.

- **Las consideraciones posteriores a la terminación del contrato**: En lo que tiene que ver con la entrega de información y la conservación de copias por parte del proveedor de servicios en la nube, la asistencia en el periodo de transición a otro proveedor, y obligaciones de destrucción de la información.
- **El contrato marco y sus anexos, identificación de las partes, el objeto del contrato, obligaciones de las partes, protección de datos de carácter personal.**[11]

Como se observa las temáticas de seguridad de la información cobran gran relevancia en este tipo de servicios, cada vez de uso más generalizado. Como referencia de una experiencia internacional se puede mencionar el caso de Brasil, donde la presidenta Dilma Rousseff, se mostró preocupada por la privacidad y confidencialidad de la información de los usuarios de internet. Por lo cual, planteó la posibilidad de que las empresas sean obligadas a almacenar todos los datos de los brasileños en servidores locales es decir, sistemas informáticos que se encuentren físicamente establecidos en ese país, de tal modo que las leyes brasileñas sobre dicha materia puedan ser aplicadas[12].

Ahora bien, se observa que a nivel mundial los esfuerzos para reforzar la ciberseguridad en los países no cesa, y es así como la OEA[13] presentó el pasado 21 de enero de 2015 en la reunión anual del Foro Económico Mundial realizada en Davos, Suiza, el programa de seguridad cibernética de la OEA para los países de América Latina y el Caribe, dado que es la región del mundo donde Internet se está expandiendo a mayor velocidad. Se presentó el trabajo que la OEA está desarrollando con muchos países de la región para hacer frente a los peligros potenciales que tienen las nuevas tecnologías y se explicó que el programa de seguridad cibernética de la OEA *"está diseñado para asistir a los gobiernos en estrategias que son adaptadas a la realidad de cada país".* En este sentido, se indicó que la seguridad cibernética requiere un enfoque de responsabilidad compartida, en la cual los Países Miembros colaboren con todas las partes interesadas y también con otros países, se busca que en la región se elabore una política integral de seguridad cibernética.

Las diferentes actividades adelantadas por el Gobierno Nacional han permitido que Colombia sea uno de los países líderes de la región en la materia y ocupe una posición destacable a nivel mundial, tal

[11] Pág. 16-25, [Rafael García]
[12] ESET LATINOAMÉRICA. *"Tendencias 2014: El desafío de la privacidad en internet".* Disponible en http://www.eset-la.com/pdf/tendencias_2014_el_desafio_de_la_privacidad_en_internet.pdf.
[13] http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-012/15

como lo presenta el Índice Global de Ciberseguridad (GCI) de la UIT[14] para el año 2014, el cual ubica al país en el noveno (9) lugar en el ranking mundial con el mismo nivel de países como Francia, España, Egipto y Dinamarca. A nivel América, Colombia ocupa el quinto lugar por encima de Chile y México en donde los aspectos más significativos evaluados fueron el legal, el organizacional y el de la generación de capacidades.

## 3. MARCO NORMATIVO APLICABLE A LA CIBERSEGURIDAD

A continuación se exponen los principales instrumentos normativos nacionales e internacionales en materia de Ciberseguridad y Ciberdefensa los cuales sirven de base para analizar la viabilidad de acoger o no mejores prácticas internacionales que sean replicables para el caso de Colombia.

### 3.1 Marco Normativo Internacional

Según lo expuesto en el CONPES 3701 de 2011 y en algunas recomendaciones técnicas sobre *"Seguridad Cibernética"* de CITEL[15], a continuación se exponen las principales normas internacionales en materia de ciberseguridad:

**Tabla No. 1. Marco Normativo Internacional**

| INSTRUMENTO | MATERIA |
|---|---|
| Convenio sobre Ciberdelincuencia del Consejo de Europa – CCC (conocido como el convenio sobre Cibercriminalidad de Budapest[16]) 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.<br><br>Único **instrumento vinculante vigente** sobre el tema en el ámbito internacional y su protocolo para la criminalización de |

[14] La UIT lanzó la Agenda sobre Ciberseguridad Global (GCA), el mecanismo de cooperación multipartita para orientarse hacia una sociedad de la información más segura y protegida, y que se focaliza en los cinco ámbitos de trabajo siguientes: Medidas legales, medidas técnicas, medidas orgánicas, capacitación, y cooperación. Estos cinco ámbitos señalados son la base de los indicadores para el IMC (GCI) http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

[15] Documento CONPES 3701 de 2011 expedido por el Departamento Nacional de Planeación – Consejo Nacional de Política Económica y Social. Bogotá 14 de julio de 2011. Página 14. Disponible en http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf.

[16] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_spanish.PDF

| INSTRUMENTO | MATERIA |
|---|---|
| | 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 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.<br><br>Es importante señalar que Colombia logró la invitación del Consejo de Europa para adherirse a la Convención de Budapest, como resultado de un proceso que inició en el año 2011 con la promulgación del Documento CONPES 3701, el cual requirió que el Ministerio de Relaciones Exteriores realizara una solicitud formal al Consejo de Europa para que Colombia fuera invitada a hacer parte de la Convención de Budapest. De esta manera, el 20 de septiembre de 2013, el Consejo de Ministros del Consejo de Europa aprobó la invitación para que Colombia adhiera a la Convención de Budapest, y sea parte del protocolo adicional relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos. A partir de esta decisión Colombia cuenta con cinco (5) años para adherir al instrumento internacional. |
| Resolución AG /RES 2004 (XXXIV-O/04) de la Asamblea General de la Organización de los Estados Americanos[17] | 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.<br><br>Estipula tres vías de acción: i) Creación de una Red Hemisférica de Equipos Nacionales de Respuesta a Incidentes de Seguridad de Computadores – **CSIRT**, cometido asignado al Comité Interamericano Contra el Terrorismo – CICTE; ii) |

[17] Es importante resaltar que parte de la Doctrina ha establecido que dichas Resoluciones y Recomendaciones hacen parte del llamado "Soft Law", como fuente formal del Derecho Internacional. Aunque., en este caso Colombia como país miembro de la

| INSTRUMENTO | MATERIA |
|---|---|
| | **Identificación y adopción de normas técnicas para una arquitectura segura de Internet**, labor desarrollada por la Comisión Interamericana de Telecomunicaciones; y iii) 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.<br><br>La estrategia integral de seguridad cibernética es descrita en esta Resolución AG/RES. 2004 (XXXIV-O/04), aprobada en la cuarta sesión plenaria del trigésimo cuarto período ordinario de sesiones de la Asamblea General de la OEA, celebrada el 8 de junio de 2004. En esta medida las Resoluciones tienen un nivel de cumplimiento diferente al que genera un Tratado o una Convención, puesto que si un País miembro de la OEA ha aprobado la Resolución a través del voto se espera que el País tenga el mismo compromiso para llevar a cabo su cumplimiento. En este caso Colombia como miembro de la Asamblea General de la OEA suscribió esta Resolución, y la fuerza vinculante de las resoluciones se refleja en la obligatoriedad que tienen los países de presentar informes y exponer resultados, en relación con lo que se ha acordado en estas.<br><br>Adicionalmente, Colombia como miembro del Comité Interamericano contra el Terrorismo (CICTE) y de la Comisión Interamericana de Telecomunicaciones (CITEL), debe sujetarse a las Resoluciones y recomendaciones que emitan estos organismos.<br><br>Finalmente es importante tener en cuenta que las Resoluciones |

OEA ratifico "La Carta de la OEA", lo que vincula al país al cumplimiento en la medida de sus posibilidades por temas presupuestales de las Resoluciones que se emitan en el marco de la asamblea general de la ONU.

| INSTRUMENTO | MATERIA |
|---|---|
| | de la OEA, no tienen el carácter vinculante de un tratado, sin embargo la Asamblea General es el órgano supremo de la OEA y todas sus manifestaciones tienen un elevado nivel político diplomático.[18] |
| 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.<br><br>De acuerdo con el artículo 3 del Tratado de creación del Tribunal de Justicia de la CAN, el esquema jurídico de la CAN es supranacional, lo que se traduce en la emisión de leyes o normas comunitarias[19], que tienen efectos directos y vinculantes en los países miembros desde la fecha de su publicación en la Gaceta Oficial del Acuerdo de Cartagena sin necesidad de requerir previa aprobación de los Congresos Nacionales para su entrada en vigencia en cada uno de los países miembros. |
| Consenso en materia de Ciberseguridad de la Unión Internacional de Telecomunicaciones - UIT, en el seno de Naciones Unidas, en desarrollo del programa de acciones de Túnez para la | Busca la promoción del examen de los conceptos internacionales pertinentes encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones.<br><br>Las Resoluciones que emita la UIT son vinculantes[20] para Colombia, puesto que a través de las Leyes 252 de 1995 y 873 |

[18] Es importante resaltar que parte de la Doctrina ha establecido que las Recomendaciones hacen parte del llamado "Soft Law", como fuente formal del Derecho Internacional.
[19] Compuestas por las Decisiones expedidas por el Consejo Andino de Ministros de Relaciones Exteriores y la Comisión de la Comunidad Andina, así como las Resoluciones expedidas por la Secretaria General de la Comunidad Andina.
[20] Respecto de algunas recomendaciones en temas específicos que emita la UIT, es importante tener en cuenta que su cumplimiento se da en la medida en que el Estado Colombiano pueda ejecutarlas de acuerdo a su presupuesto.

| INSTRUMENTO | MATERIA |
|---|---|
| sociedad de la información de 2005 | de 2004, se aprobó la constitución de la UIT y el Convenio de la UIT, así como las enmiendas posteriores que se han realizado. |
| 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 (UNGA). (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 emitidas hasta el 2 de diciembre de 2008.<br><br>Las Resoluciones de la Asamblea General de la ONU, como las que afectan cuestiones presupuestarias, asuntos internos o instrucciones a órganos de rango inferior son vinculantes, sin embargo las recomendaciones de la Asamblea General y las Resoluciones fundadas en estas, se cumplen en la medida que el Estado pueda ejecutarlas de acuerdo a su presupuesto. |
| Directiva 2006/24 de la Unión Europea | La Directiva 2006/24 establecía la conservación de datos en la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y fue el referente aplicado por los países miembros hasta el año 2014. Esta directiva fue declarada inválida por el Tribunal de Justicia de la Unión Europea en Abril de 2014 dado que imponía a los países miembros la obligación de adoptar en las legislaciones internas la conservación de datos que se cursan en el tráfico de las comunicaciones[21], por considerar que dicha medida vulnera los derechos fundamentales al respeto de la vida privada y a la protección de datos de carácter personal. |
| Pronunciamientos de Principios | Resoluciones UNGA: 55/63 y 56/121 sobre la lucha contra el |

[21] Está Directiva determina que por conservación de datos se entiende: con respecto a la telefonía de red fija y a la telefonía móvil: i) el número de teléfono de llamada, ii) el nombre y la dirección del abonado o usuario registrado; 2) con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet: i) la identificación de usuario asignada, ii) la identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía, iii) el nombre y la dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo Internet (IP), una identificación de usuario o un número de teléfono.

| INSTRUMENTO | MATERIA |
|---|---|
| Generales. UNGA | uso delictivo de tecnologías de información; 57/239, 58/199 y 64/211 sobre la creación de una cultura mundial de seguridad cibernética y la protección de infraestructuras críticas de información; Cumbre Mundial sobre la Sociedad de la Información (CMSI), Declaración de Principios y Orden del Día de la Fase de Túnez (en particular la línea de acción C5).<br><br>Estas son normas o principios generales, que no constituyen reglas y no son vinculantes, sin embargo estos actos o instrumentos jurídicos sin carácter obligatorio, son incardinados de una forma u otra, en el sistema de fuentes del Derecho Internacional *(Soft Law).* |

Es importante resaltar que en el 2013 el Consejo de Ministros del Consejo de Europa aprobó la solicitud de adhesión de Colombia al Convenio de Budapest, en este sentido, las acciones y requisitos necesarios para lograr dicho objetivo deben considerarse dentro de la Estrategia Nacional de Ciberseguridad, teniendo en cuenta además las recomendaciones de expertos nacionales e internacionales y las resoluciones de la OEA a través de sus organismos especializados como CICTE y CITEL en temas de Ciberseguridad y Cibercriminalidad. Así mismo, deben tenerse en cuenta las disposiciones establecidas en la Decisión 587 de la CAN, las cuales son de carácter vinculante para Colombia.

### 3.2 Marco Normativo Nacional

El Gobierno Nacional ha expedido algunas normas que consagran diferentes medidas relacionadas con la Ciberseguridad y Ciberdefensa, entre las que se destacan:

**Tabla No. 2. Marco jurídico colombiano**

| NORMA | CONTENIDO |
|---|---|
| **Constitución Nacional** | Art. 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.<br><br>En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. |

| NORMA | CONTENIDO |
|---|---|
| | La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.<br><br>Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley. |
| **Ley 527 de 1999 (Comercio Electrónico)** | Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. |
| **Ley 679 de 2001 (Pornografía y explotación sexual con menores)** | Esta Ley contempla en el artículo 4, un sistema de autorregulación, en virtud del cual el gobierno nacional, por intermedio del Ministerio de Comunicaciones – hoy MinTIC-, promoverá e incentivará la adopción de sistemas de autorregulación y códigos de conducta eficaces en el manejo y el aprovechamiento de redes globales de información, estos códigos se elaboraran con la participación de organismos representativos de los proveedores y usuarios de servicios de redes globales de información.<br><br>Por otra parte, esta Ley contempla en el artículo 7, para los proveedores o servidores, administradores y usuarios de redes globales de información, determinadas prohibiciones como: alojar en su propio sitio imágenes, textos o archivos que impliquen actividades sexuales con menores; alojar en su propio sitio material pornográfico que contenga imágenes o videos, en los cuales las personas filmadas o fotografiadas sean menores de edad; alojar en sitio links sobre páginas que remitan a temáticas de pornografía infantil.<br><br>Finalmente, la Ley en el artículo 8 contempla que los proveedores, administradores y usuarios de redes globales de información deberán: denunciar la difusión de material pornográfico con menores de edad. |
| **Ley 1266 de 2008 (Habeas Data)** | Contempla las disposiciones generales en relación al Derecho de Habeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. |
| **Ley 1273 de 2009 (Delitos Cibernéticos)** | En el año 2009 se expide la Ley 1273 "*Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos" – y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones".* |

| NORMA | CONTENIDO |
|---|---|
| | Se crean los siguientes tipos penales:<br>Capítulo I – "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", este capítulo tipifica las siguientes conductas penales: Acceso Abusivo a un sistema informático, obstaculización ilegítima de sistema informático o de red de telecomunicación, interceptación de datos informáticos, daño informático, uso de software malicioso, violación de datos personales, suplantación de sitios web para capturar datos personales.<br><br>Capítulo II – "De los atentados informáticos y otras infracciones", este capítulo tipifica las siguientes conductas: hurto por medios informáticos y semejantes, transferencia no consentida de activos. |
| **Ley 1336 de 2009 (Explotación, pornografía y el turismo sexual con niños)** | A través de esta Ley *"se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes".* Esta Ley establece dos medidas para contrarrestar la explotación sexual y la pornografía infantil que se relacionan tangencialmente con las Tecnologías de la Información y las Comunicaciones, en primer lugar establece en el Artículo 4 (autorregulación de café internet – Códigos de conducta) que todo establecimiento abierto al público que preste servicios de internet o de café internet deberá colocar en un lugar visible un reglamento de uso público adecuado de la red, y deberá indicar que la violación a este genera la suspensión del servicio al usuario.<br><br>Finalmente, en el artículo 19 se establece que el documento de criterios de clasificación de páginas en internet con contenidos de pornografía infantil y de recomendaciones al gobierno será actualizado cada dos años, a fin de revisar la vigencia doctrinal de sus definiciones, actualizar los criterios sobre tipos y efectos de la pornografía infantil, con el fin de asegurar la actualidad de los marcos tecnológicos de acción. |
| **Ley 1480 de 2011 (Estatuto del Consumidor - Comercio electrónico y publicidad)** | La Ley 1480 en el artículo 5, incluye en la definición de las ventas a distancia, aquellas que se realizan a través del comercio electrónico.<br>El artículo 26 de esta Ley, consagra que la SIC determinará las condiciones mínimas bajo las cuales operar la información pública de precios de los productos que se ofrezcan a través de cualquier medio electrónico.<br><br>Adicionalmente, el artículo 27 establece que el consumidor tiene derecho a exigir a costa del productor o proveedor constancia de toda operación de consumo que realice. La factura o su equivalente, expedida por cualquier medio físico, **electrónico o similar** podrán hacer las veces de constancia. |

| NORMA | CONTENIDO |
|---|---|
| **Ley 1453 de 2011 (Estatuto de seguridad ciudadana)** | El Art. 236 establece que cuando el fiscal tenga motivos razonables, para inferir que el indicado o imputado está transmitiendo o manipulando datos a través de las redes de telecomunicaciones, ordenará a la policía la retención, aprehensión o recuperación de dicha información, equipos terminales, dispositivos o servidores que pueda haber utilizado cualquier medio de almacenamiento físico o virtual, análogo o digital, para que expertos en informática forense, descubran, recojan, analicen y custodien la información que recuperen; lo anterior con el fin de obtener elementos materiales probatorios y evidencia física o realizar la captura del indiciado, imputado o condenado.<br><br>La aprehensión que trata este artículo se limitará exclusivamente al tiempo necesario para la captura de la información en él contenida. Inmediatamente se devolverán los equipos incautados, de ser el caso. |
| **Ley 1581 de 2012 (Habeas Data)** | *"Por la cual se dictan disposiciones generales para la protección de datos".*<br>Esta Ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada, sin embargo a los datos financieros se les continúa aplicando la Ley 1266 de 2008, excepto los principios. |
| **Ley 1621 de 2013 (Marco jurídico que para desempeño de funciones de los organismos de inteligencia y contrainteligencia– Protección a las bases de datos)** | Esta Ley tiene por objeto fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir adecuadamente con su misión constitucional y legal, así mismo esta Ley establece los límites y fines de las actividades de inteligencia y contrainteligencia, los mecanismos de control y supervisión y la regulación de la protección a las bases de datos. En el marco de la Ley hay diversas autoridades que manejan inteligencia tales como UIAF, POLFA, DIPOL son organismos con función de policía judicial.<br><br>El Art. 17 establece obligaciones en relación al monitoreo del espectro y la interceptación de comunicaciones.<br>El Art. 44 consagra el deber de colaboración de los operadores de comunicaciones para entregar a los organismos de inteligencia determinados datos como: el historial de comunicaciones, los datos técnicos de identificación de los usuarios, así como la localización de las celdas en que se encuentran las terminales.<br><br>Adicionalmente, los operadores se encuentran obligados a informar al MinTIC cualquier modificación en la tecnología de sus redes que impida la interceptación de comunicaciones. |
| **Decreto 1727 de 2009** | Se determina la forma en la cual los operadores de los bancos de |

| NORMA | CONTENIDO |
|---|---|
| **(Habeas Data)** | datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información. |
| **Decreto 2952 de 2010 (Habeas Data)** | Este Decreto reglamenta los artículos 12 y 13 de la Ley 1266 de 2008, en este sentido establece que con fundamento en el principio constitucional de solidaridad surgen obligaciones a cargo del Estado y de los ciudadanos, en virtud de las cuales cuando se presenten situaciones de fuerza mayor, es posible otorgar a las víctimas de secuestro, desaparición forzada y personas secuestradas, debido a su estado de debilidad manifiesta, un tratamiento diferenciado en la administración de su información financiera, crediticia y comercial. |
| **Decreto 1704 de 2012 (Interceptación legal de comunicaciones)** | Este Decreto determina que la interceptación legal de comunicaciones, es un mecanismo de seguridad pública que busca optimizar la labor de investigación de los delitos que adelantan las autoridades y organismos de inteligencia.<br><br>De esta manera, se determina que los PRST que desarrollen su actividad comercial en el territorio nacional, deben implementar y garantizar en todo momento la infraestructura tecnológica necesaria que provea los puntos de conexión y de acceso a la captura del tráfico de las comunicaciones que cursen por sus redes, para que los organismos con funciones permanentes de policía judicial cumplan, previa autorización del Fiscal General de la Nación, con todas las labores inherentes a la interceptación de las comunicaciones requeridas.<br><br>Adicionalmente, el Decreto establece que una vez cumplido los requisitos legales, los PRST deben suministrar a la Fiscalía General de la Nación de forma inmediata, los datos del suscriptor, tales como identidad, dirección de facturación y tipo de conexión, los cuales deben estar actualizados y deben ser conservados por 5 años.<br><br>En el año 2012 se interpuso una demanda de Nulidad contra la expresión *"o demás autoridades competentes"* contenida en el artículo 4 del Decreto 1704/2012. En escrito separado se solicitó la suspensión provisional de la expresión mencionada, la cual fue concedida mediante Auto del 31 de julio de 2013, y confirmada en el resuelve del recurso de súplica interpuesto por el MinTIC, el 3 de abril de 2014.<br><br>Por lo anterior, actualmente se encuentra suspendida únicamente la expresión" o demás autoridades competentes" contenida en el artículo 4 del Decreto 1704. No obstante, es de notar que la Ley 1453 de 2011 (Reforma al Código Penal) fue declarada exequible, y el artículo 52 que modifica el art. 235 de la Ley 906 de 2004, dispone la interceptación de comunicaciones que se cursen por cualquier red, según orden de |

| NORMA | CONTENIDO |
|---|---|
| | fiscal. |
| **Decreto 2758 de 2012 (Modifica la Estructura del Misterio de Defensa)** | Se reestructura la organización del Ministerio de Defensa, en el sentido de asignar al despacho del Viceministro la función de formular políticas y estrategias en materia de ciberseguridad y ciberdefensa.<br><br>Adicionalmente le encarga a la Dirección de Seguridad Pública y de Infraestructura, la función de implementar políticas y programas que mantengan la seguridad pública y protejan la infraestructura, así como hacerle seguimiento a la gestión relacionada con el riesgo cibernético en el sector defensa y diseñar el plan estratégico sectorial en materia de ciberseguridad y ciberdensa. |
| **Decreto 1377 de 2013 (Habeas Data)** | "A través de este Decreto se reglamenta parcialmente la Ley 1581 de 2012".<br>El decreto tiene como objetivo facilitar la implementación y el cumplimiento de la Ley 1581 de 2012, reglamentando aspectos particulares relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, además consagra políticas de tratamiento de los responsables y encargados. |
| **Decreto 0032 de 2013 (Creación de la Comisión Nacional Digital y de Información Estatal)** | El Ministerio de TIC en cumplimiento de los lineamientos señalados en el Documento CONPES 3701 DE 2011 , creo a través de este Decreto, la Comisión Nacional Digital y de Información Estatal cuyo objeto es la coordinación y orientación superior de la ejecución de funciones y servicios públicos relacionados con el manejo de la información pública, el uso de infraestructura tecnológica de la información para la interacción con los ciudadanos y el uso efectivo de la información en el Estado Colombiano.<br><br>Adicionalmente, dicha Comisión debe emitir los lineamientos rectores del Grupo de Respuesta a Emergencias Cibernéticas de Colombia del Ministerio de Defensa Nacional y asesorar al Gobierno Nacional en materia de políticas para el sector de ciberseguridad. |
| **Decreto 333 de 2014 (Habeas Data)** | Este Decreto define el régimen de acreditación de las entidades de certificación en desarrollo de lo que consagra el Articulo 160[22] del Decreto Ley 19 de 2012. |

[22] Decreto Ley 19 de 2012. Artículo 160: *Podrán ser entidades de certificación, las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero y las cámaras de comercio, que cumplan con los requerimientos y sean acreditados por el Organismo Nacional de Acreditación conforme a la reglamentación expedida por el Gobierno Nacional. El Organismo Nacional de Acreditación de Colombia suspenderá o retirará la acreditación en cualquier tiempo, cuando se establezca que la entidad de certificación respectiva no está cumpliendo con la reglamentación emitida por el Gobierno Nacional, con base en las siguientes condiciones: a. Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como entidad de certificación; b. Contar con la capacidad y elementos técnicos necesarios para la generación de firmas digitales, la emisión de certificados sobre la autenticidad de las mismas y la conservación de mensajes de datos en los términos establecidos en esta ley; c. Los representantes legales y administradores no podrán ser personas que hayan sido condenadas a*

| NORMA | CONTENIDO |
|---|---|
| | |
| **Decreto 857 de 2014** | Por medio del cual se reglamenta la Ley estatutaria 1621 de 2013, que establece el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, para cumplir con su misión constitucional y legal. Adicionalmente, establece la reserva legal, los niveles de clasificación y el sistema para la designación de los niveles de acceso a la información y clasificación de documentos. |
| **Resolución CRC 3067 de 2011 "Por la cual se definen los indicadores de calidad para los servicios de telecomunicaciones y se dictan otras disposiciones"** | Está Resolución establece en el artículo 2.3, que los PRST que ofrezcan acceso a internet deben utilizar los recursos técnicos y logísticos tendientes a **garantizar la seguridad de la red y la integridad del servicio**, para evitar la interceptación, interrupción e interferencia del mismo. Para lo cual, deben informar en su página web las acciones adoptadas en relación con el servicio prestado al usuario final, tales como el uso de firewalls. Filtros antivirus y la prevención del spam, phishing, malware entre otros; no obstante la responsabilidad de los PRST no cubre los equipos del cliente, puesto que los mismos son controlados directamente por el usuario del servicio.<br><br>Adicionalmente, los PRST que ofrezcan acceso a internet deberán **implementar modelos de seguridad**, de acuerdos con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso, en línea con los marcos de seguridad definidos por la UIT, en lo relativo a las recomendaciones pertenecientes a las series X.800, y en relación con los siguientes aspectos: autenticación (UIT X.805 y UIT X.811), acceso (UIT X.805 y UIT X.812), no repudio (UIT X.805 y UIT X.813), confidencialidad de datos (UIT X.805 y UIT X.814), integridad de datos (UIT X.805 y UIT X.815) y disponibilidad (UIT X.805).<br><br>Finalmente se establece, los PRST a través de redes móviles, deberán implementar **modelos de seguridad que eviten el acceso no autorizado, la interrupción, el repudio o la interferencia deliberada de la comunicación**, utilizando modelos de cifrados, firmas digitales y controles de acceso descritos en las recomendaciones UIT X.1121 y X.1122. |
| **Resolución CRC 3502 de 2011 (Neutralidad de Internet)** | A través de la Resolución 3502 de 2011, se establecen condiciones regulatorias relativas a la neutralidad en internet, en cumplimiento de lo establecido en el artículo 56 de la Ley 1450 de 2011 (Plan Nacional de Desarrollo 2010 – 2014). Esta resolución, contempla en el artículo 3 |

*pena privativa de la libertad, excepto por delitos políticos o culposos; o que hayan sido suspendidas en el ejercicio de su profesión por falta grave contra la ética o hayan sido excluidas de aquélla. Esta inhabilidad estará vigente por el mismo período que la ley penal o administrativa señale para el efecto.*

| NORMA | CONTENIDO |
|---|---|
| | los principios de libre elección, no discriminación, transparencia e información, que deben aplicar los PRST que prestan el servicio de acceso a internet. |
| **Resolución SIC No. 76434 de 2012 (Habeas Data)** | Resolución expedida por la SIC, por medio de la cual se imparten instrucciones relativas a la protección de datos personales, en particular acerca del cumplimiento de la Ley 1266 de 2008, sobre reportes de información financiera, crediticia, comercial de servicios y la proveniente de terceros países. |
| **Resolución 3933 de 2013 Del Ministerio de Defensa (Crea y organiza grupos internos de trabajo)** | Creó el Grupo colCERT y asignó funciones a la dependencia de la Dirección de Seguridad Pública y de Infraestructura del Ministerio de Defensa Nacional, respecto a promover el desarrollo de capacidades locales/sectoriales para la gestión operativa de los incidentes de ciberseguridad y ciberdefensa en las infraestructuras críticas nacionales, el sector privado y la sociedad civil. |

Respecto al marco jurídico nacional expuesto, es importante considerar que para formular la nueva Estrategia Nacional de Ciberseguridad y Ciberdefensa, se debe tener en cuenta la actual legislación en materia de protección de datos personales[23], ciberdelitos[24], y en materia procesal penal, para identificar en qué aspectos particulares se pueden requerir modificaciones.

## 4. ESTRATEGIA DE CIBERSEGURIDAD Y CIBERDEFENSA EN COLOMBIA: CONPES 3701 DE 2011

A continuación se parte del marco de referencia en materia de Ciberseguridad y Ciberdefensa planteado en Colombia en el año 2011.

### 4.1 Actores y responsabilidades

El gobierno nacional a través del CONPES 3701 de 2011 definió la creación de tres grupos orientados a proteger a los cibernautas y los sistemas de información nacional, así:

- Grupo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT,
- Comando Conjunto Cibernético de las Fuerzas Militares, y

[23] Ley 1266 de 2008, Ley 1581 de 2012, Decretos 1727 de 2009, 2952 de 2010 y 1377 de 2013.
[24] La Ley 1273 de 2009, consagra diferentes tipos penales en materia de ciberdelitos, no obstante de acuerdo a las recomendaciones de expertos internacionales, es necesario que la Ley de ciberdelitos en Colombia integre y amplié delitos contra los derechos de autor, contra el derecho de habeas data y que haga alusión al acceso transfronterizo de datos informáticos almacenados.

- Comisión Intersectorial, en la cual participan de una manera integrada el Ministerio de Defensa Nacional, Ministerio de Justicia y del Derecho, Ministerio de Tecnologías de la Información y las Comunicaciones y otras entidades como SENA, Consejo Superior de la Judicatura, la Comisión de Regulación de Comunicaciones y el DAS (hoy, Agencia Nacional de Inteligencia) .

**Gráfico No. 5**


Fuente: MinDefensa

A su vez, dentro del citado CONPES se especifican los principales actores para llevar acabo el desarrollo de la estrategia de ciberseguridad y ciberdefensa, indicando además las actividades que debe adelantar cada uno, información que se encuentra descrita en la Tabla No. 3.

**Tabla No. 3. Mapa de actores y responsabilidades - CONPES 3701 de 2011**

| Entidad | Actividades/Responsabilidades | Otras entidades |
|---|---|---|
| DNP DEPARTAMENTO NACIONAL DE PLANEACIÓN | Aprobar los lineamientos de Política para el desarrollo e impulso de la estrategia de ciberseguridad y la Ciberdefensa, presentados en el CONPES | |
| MinDefensa Ministerio de Defensa Nacional | Adoptar (o crear) el mecanismo de coordinación intersectorial más adecuado para emitir los lineamientos rectores del colCERT. En caso de no existir uno, se solicita su creación. | |
| | Crear el Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT. | |
| | Una vez creado el colCERT, emitir los modelos de seguridad en el ciberespacio[25] que minimicen el nivel de riesgo al que las entidades están expuestas. | |
| | Crear el Centro Cibernético Policial – CCP. | |
| | Crear el Comando Conjunto Cibernético – CCOC. | |
| | Realizar en coordinación con MINTIC estudios en seguridad de la información, así como la identificación de la infraestructura crítica nacional. | MINTIC |
| | Diseñar las campañas de sensibilización y concienciación en temas de seguridad cibernética, en coordinación con MINTIC. | MINTIC |
| | 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 | |
| | Adelantar un plan de capacitación en temas de seguridad de la información para los funcionarios del Estado, con el apoyo de organismos internacionales. | |

[25] Es importante mencionar que el Documento CONPES 3701 de 2011, definió al ciberespacio en los siguientes términos: *"Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización de la electrónica, la informática y la cibernética".* Está definición la adopta de acuerdo a lo que establece la Real Academia de la Lengua Española. Documento disponible en http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf . Pág. 14.

| Entidad | Actividades/Responsabilidades | Otras entidades |
|---|---|---|
| | Diseñar e implementar planes de capacitación en lo referente a seguridad informática, investigación y judicialización de delitos informáticos, para policía judicial. | |
| | Solicitar al Ministerio del Interior y de Justicia realizar en coordinación con el Ministerio de Defensa Nacional y el Ministerio de Tecnologías de la Información y las 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[26], identificando las dificultades de interpretación y aplicación. | MINTIC, MinDefensa y DAS |
| MinTIC Ministerio de Tecnologías de la Información y las Comunicaciones | Adoptar (o crear) el mecanismo de coordinación intersectorial más adecuado para emitir los lineamientos rectores del colCERT. | |
| | Acompañar (junto con **CRC**) a MinDefensa en la conformación y el desarrollo de las actividades del colCERT | **CRC**, MinDefensa |
| | 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. | MinJusticia, MinTIC, DAS |
| | Emitir un documento con las directrices en temas de seguridad de la información basada en estándares internacionales, que deberán ser implementadas por las entidades del sector público. | |
| | Facilitar los canales institucionales para que el colCERT pueda realizar la sensibilización y concienciación en temas de seguridad cibernética. | |

[26] 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). Extraído del Conpes 3701 de 2011.

| Entidad | Actividades/Responsabilidades | Otras entidades |
|---|---|---|
| | Diseñar e implementar planes de capacitación en lo referente a seguridad informática, investigación y judicialización de delitos informáticos, para policía judicial. | MinTIC, MinDefensa, DAS |
| | 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. | MinEducación, SENA |
| | Elaborar 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. | MinJusticia, MinTIC, MinDefensa |
| | 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 | MinTIC |
| | 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. | |
| | Destinar recurso humano con conocimientos técnicos y/o jurídicos e n e l tema de seguridad de la información y ciberseguridad, para apoyar la ejecución de actividades del colCERT. | MinTIC, DAS |

| Entidad | Actividades/Responsabilidades | Otras entidades |
|---|---|---|
| | 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. | MinDefensa, MinTIC |
| | 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 e l marco normativo adecuado para la ciberseguridad, la ciberdefensa y la seguridad de la información. | MinDefensa, MinTIC |
| Departamento Administrativo de Seguridad, en proceso de Supresión República de Colombia | Destinar recurso humano con conocimientos técnicos y/o jurídicos e n e l tema de seguridad de la información y ciberseguridad, para apoyar la ejecución de actividades del colCERT. | MinTIC, MinJusticia |
| | Diseñar e implementar planes de capacitación e n lo referente a seguridad informática, investigación y judicialización de delitos informáticos, para policía judicial. | MinTIC, MinDefensa |
| FISCALÍA GENERAL DE LA NACIÓN | Diseñar e implementar planes de capacitación sobre temas de investigación y judicialización de delitos informáticos, para policía judicial, jueces y fiscales. | Consejo Superior de la Judicatura |
| Cancillería 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. | |
| | 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 MinDefensa y el MinTIC. En caso de que | |

| Entidad | Actividades/Responsabilidades | Otras entidades |
|---|---|---|
| | el estudio produzca una recomendación positiva, iniciar los trámites de adhesión al instrumento que corresponda. | |

### 4.2 Principales Avances

Es importante destacar que varias de las políticas trazadas en el documento CONPES 3701 de 2011 se materializaron con la expedición de normas desde diferente campos.

Según indica el Departamento Nacional de Planeación - DNP encargado del seguimiento a los lineamientos de política para ciberdefensa y ciberseguridad, uno de los aportes importantes en la estrategia estuvo a cargo del Ministerio de Defensa al expedir el Decreto No. 2758 de 2012, que asignó funciones en materia de ciberseguridad y ciberdefensa a la **Dirección de Seguridad Pública y de Infraestructura**, y mediante la expedición de la Resolución 3933 de 2013, que creó el grupo de Respuesta a Emergencias Cibernéticas -**Grupo colCERT-** y asignó funciones, a la dependencia de la Dirección de Seguridad Pública y de Infraestructura del Ministerio de Defensa Nacional. De igual manera se emitió el Decreto No. 32 de 2013 por el cual se creó la **Comisión Nacional Digital y de Información Estatal**. Además, el Ministerio de Defensa constituyó e inició la operación del Comando Conjunto Cibernético de las Fuerzas Militares, y se conformó el Centro Cibernético de la Policía –CCP- dentro de la Dirección de investigación criminal e Interpol. Así mismo Colombia participa en una iniciativa multinacional liderada por Interpol para identificar, investigar y arrestar a usuarios que a través de foros en línea están involucrados en delitos de abuso y pornografía de menores, cabe resaltar que el personal del CCP ha recibido capacitación en investigación cibernética y análisis forense digital por parte del Departamento de Estado de los Estados Unidos (DS/ATA), FBI y por los Gobiernos de España y Francia.

Ahora bien, con el fin de fomentar la resiliencia de los sistemas internos y la integridad de la información, la Policía Nacional ha desarrollado sus sistemas internos para la gestión de la seguridad de la información en cumplimiento con la norma ISO 27001. Se resalta también la expedición de

normas relativas a la protección de los datos personales, como la Ley 1581 de 2012[27] y el Decreto 1377 de 2013[28] que reglamentó dicha Ley.

Por otra parte, en el año 2012 el Ministerio de TIC expidió el Decreto 1704 que determina las pautas a los proveedores de telecomunicaciones para que la Fiscalía pueda realizar actividades de interceptación legal de las comunicaciones.

Se destaca en materia de ciberseguridad la expedición de la Ley 1621 de 2013, que consagra el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal. Esta Ley fue reglamentada por el Decreto 857 de 2014, el cual delimita las funciones de los organismos, dependencias y personal que realizan actividades de inteligencia y contrainteligencia, y establece varios criterios para la protección de los datos recolectados en las labores de inteligencia y contrainteligencia.

En lo relativo a la identificación de Infraestructuras Críticas, esta es una tarea en cabeza del Comando Conjunto de Operaciones Cibernéticas – CCOC-del Ministerio de Defensa. A partir del Decreto 2758 de 2012 y la Resolución 3933 de 2013, expedidos por el Ministerio de Defensa Nacional, se asignan a la **Dirección de Seguridad Pública y de Infraestructura** de ese Ministerio, la función de promover el desarrollo de capacidades locales/sectoriales para la gestión operativa de los incidentes de Ciberseguridad y Ciberdefensa en las infraestructuras críticas nacionales, del sector privado y la sociedad civil.

Para la identificación de infraestructuras críticas se han establecido metas específicas, que van desde el establecimiento de una red de contactos, hasta el diseño, desarrollo y consolidación de guías a través de las cuales se definan lineamientos generales que permitan contar con procedimientos comunes para mejorar la seguridad de los sistemas informáticos asociados incluyendo la infraestructura de las telecomunicaciones. Las guías han sido divididas en 5 categorías diferentes que comprenden la Gestión de Activos, Gestión de Vulnerabilidades, Gestión de Riesgos, Gestión de Incidentes de Seguridad y Gestión de Continuidad del Negocio, las cuales serán implementadas a manera de piloto a lo largo del año 2015.

Es importante aclarar que dicha identificación no se limita al sector de telecomunicaciones y TIC, sino que considera sectores como petroquímico, hídrico, minero, educativo y alimentos, entre otros. El

[27] Ley Estatutaria por medio de la cual se dictan disposiciones generales para la protección de datos personales.
[28] "Por el cual se reglamenta parcialmente la Ley 1581 de 2012", y se establecen diversas disposiciones en materia de protección de datos.

ejercicio de identificación de infraestructuras críticas ha tenido en cuenta y desarrollado un análisis de las experiencias internacionales, considerando países como Estados Unidos, Canadá, Reino Unido, España, Chile y Australia. Se planea que en el término de un año, se defina la normatividad asociada a las infraestructuras críticas en el país a partir de un trabajo intersectorial, en el que la CRC ha iniciado su participación.

De otro lado, la Comisión de Regulación de Comunicaciones mediante la Resolución CRT 2058 de 2009, posteriormente incorporada en la Resolución CRC 3066 de 2011, artículos 8, 19, 20 y 36, estableció las disposiciones mínimas en materia de seguridad de redes de telecomunicaciones de acuerdo a la recomendaciones de la UIT-T en la materia en cumplimiento de aspectos definidos en el CONPES 3071.

Por otra parte, la CRC expidió la Resolución 3067 de 2011, en la cual en su artículo 2.3 Seguridad de la red, determina que los PRST deben utilizar los recursos técnicos y logísticos tendientes a garantizar la seguridad en la red y la integridad del servicio, de esta manera deberán informar en su página web las acciones adoptadas en relación con el servicio prestado al usuario final, tales como el uso de firewalls, filtros antivirus y la prevención del spam, phishing, malware entre otros.

Adicionalmente, los PRST que ofrezcan acceso a internet deben 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, en línea con los marcos de seguridad definidos por la UIT, en lo relativo a las recomendaciones pertenecientes a las series X.800, y en relación con los siguientes aspectos: autenticación (UIT X.805 y UIT X.811), acceso (UIT X.805 y UIT X.812), no repudio (UIT X.805 y UIT X.813), confidencialidad de datos (UIT X.805 y UIT X.814), integridad de datos (UIT X.805 y UIT X.815) y disponibilidad (UIT X.805).

Finalmente, la Resolución CRC 3067 establece que los PRST a través de redes móviles, deberán implementar modelos de seguridad que eviten el acceso no autorizado, la interrupción, el repudio o la interferencia deliberada de la comunicación, utilizando modelos de cifrados, firmas digitales y controles de acceso descritos en las recomendaciones UIT X.1121 y X.1122.

### 4.3 Retos en la actualización de la Estrategia Nacional de Ciberseguridad y Ciberdefensa

En atención al llamado del Gobierno Nacional de crear una alta comisión para estudiar la estrategia de seguridad cibernética del país, los Ministerios de TIC, Justicia y Defensa realizaron varios encuentros con expertos nacionales e internacionales para construir una hoja de ruta sobre cómo se debe proteger el Estado de los delitos a través de Internet. Entre los temas abordados durante el 2014,

surgió el consenso de actualizar el Documento CONPES 3701 de 2011, cuyo objetivo era formular la nueva Estrategia Nacional de Ciberseguridad y Ciberdefensa, para contrarrestar el incremento de las amenazas informáticas que afectan al país.

Con el objetivo principal de conocer la percepción que se tiene por parte del público en general y de los principales actores del sector acerca de los niveles de seguridad del uso de las TIC, las actividades adelantadas en el tema de ciberseguridad y ciberdelincuencia que amenazan al país, el Ministerio TIC adelantó una estrategia de participación y consulta pública del Plan Vive Digital II, llevada a cabo durante un periodo aproximado de 30 días en el tercer trimestre del año 2014, comentarios que podían ser allegados directamente mediante la página web www.mintic.gov.co, o a través de Facebook en el enlace https://www.facebook.com/MinisterioTIC.Colombia, dentro de la discusión de las temáticas propuestas a desarrollar dentro del Plan Vive Digital II en la búsqueda de lograr ser más efectivos en cumplir las metas propuestas. En dicha consulta[29] se encontraron los siguientes aspectos y recomendaciones que apuntan a aumentar los niveles de Ciberseguridad del país:

- Protección de datos personales, garantizar la seguridad en la disponibilidad, confidencialidad e integridad de la información.
- Acción coordinada entre entidades como Min-TIC, Min-Defensa, Fiscalía, Min-Justicia y conjunta con entes Internacionales
- Impartir formación académica sobre seguridad informática en todos los niveles jerárquicos en las entidades públicas así como Sistemas de Gestión de Seguridad (ISO 27001:2013).
- Definir mecanismos de control y trazabilidad tecnológica en el uso de las TIC.
- Crear sistema sancionatorio que las entidades puedan aplicar a delitos informáticos incluyendo la difusión de software malintencionado, y los hacker de e-mail y redes sociales.
- Programas de sensibilización ciudadana sobre las consecuencias en actos delictivos informáticos y el uso responsable del Internet.
- Seguimiento constante a las redes que prestan el servicio de internet para medir el nivel de vulnerabilidad y tomar acciones correctivas.
- Formación en temas como Hacking ético e informática forense para detectar posibles ataques a las redes del país.
- Fortalecer y dar a conocer en mayor medida entidades como el ColCERT y la Policía de delitos informáticos así como demás entidades que participan en temas relacionados con Ciberseguridad

[29] En la consulta realizada referente a Ciberseguridad, dentro del componente de Regulación, se recibieron en total 59 comentarios, participación de 39 personas, y los perfiles relacionados a los comentarios fueron Estudiantes, Profesionales, Universidades y ONG.

Ahora bien, en el marco del *"Foro de Seguridad y Defensa Cibernética: una estrategia país"*[30] realizado en 2014, el Ministerio de TIC presentó la formulación y desarrollo de una hoja de ruta la cual sirva de apoyo y bases en la elaboración de la nueva estrategia de Ciberseguridad nacional que se espera sea implementada en el año 2015. La estrategia planteada[31] considera cuatro ejes de acción:

**I.** Gobernabilidad e Institucionalidad,
**II.** Fortalecimiento de capacidades,
**III.** Cooperación nacional e internacional,
**IV.** Adecuación del Marco jurídico y normativo

El modelo recoge las recomendaciones de expertos nacionales e internacionales, entre las cuales se plantearon: crear una Agencia Nacional de Seguridad Cibernética adscrita a la Presidencia de la República; realizar un inventario de activos críticos del Estado; crear políticas a largo plazo para afrontar el desafío tecnológico, y capacitar a funcionarios judiciales en ciberdelitos.

Asimismo, se sugirió crear centros de pensamiento, innovación, excelencia y *cluster* de la industria de TI, crear CSIRT sectoriales (Grupos de Respuesta a Incidentes en Seguridad de Computo), crear un reporte nacional de incidentes y una red de alertas, aumentar la cooperación internacional con la adhesión al convenio de Budapest y, armonizar la legislación en materia de inteligencia y privacidad.[32]

De acuerdo con los ejes planteados por el Ministerio de Tecnologías de la Información y las Comunicaciones, se ha analizado el desarrollo de diversas acciones que le den curso al nuevo planteamiento estratégico. Entre las labores necesarias a implementar, se han considerado las siguientes líneas de acción:

i) la creación de planes de continuidad,
ii) la integración y alineación de las capacidades en ciberdefensa de las diferentes entidades del gobierno, a través de las cuales se haga frente a las amenazas y ataques cibernéticos,
iii) la protección de la infraestructura crítica nacional, y
iv) el fortalecimiento del ColCert y el CSIRT, extendiendo además su alcance a operaciones de seguridad Civil haciendo uso de mecanismos como el monitoreo de amenazas e incidentes de seguridad.

---

[30] http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf
[31] Consultado de: http://www.ccit.org.co/index.php/noticias/item/como-avanza-el-pais-en-materia-de-ciberseguridad-y-ciberdefensa
[32] http://www.ccit.org.co/index.php/noticias/item/como-avanza-el-pais-en-materia-de-ciberseguridad-y-ciberdefensa

Para ello se ha considerado necesario contar con las herramientas, definición de procedimientos y una correcta administración y gestión de la información, de tal forma que se tengan los insumos necesarios para dar el tratamiento adecuado a las amenazas que sean detectadas, bajo los lineamientos del Grupo de Arquitectura de TI del Ministerio de TIC.

Por otra parte, se adelanta la revisión de la normatividad existente con el fin de determinar su vigencia y pertinencia con la estrategia planteada. Dicho análisis considera los requerimientos normativos para soportar las líneas de acción propuestas.

A continuación se expondrán las principales recomendaciones que han realizado diferentes organismos internacionales para el fortalecimiento de las capacidades institucionales de Ciberdefensa y Ciberseguridad:

## 4.4 Recomendaciones de la Organización de Estados Americanos (OEA)[33]

A continuación se resumen las recomendaciones presentadas por la OEA al gobierno colombiano, luego de la misión de 2014. Las mismas se agrupan en ocho puntos o ejes que se formularon teniendo en cuenta los problemas específicos de seguridad nacional que enfrenta Colombia, y las mismas fueron realizadas reconociendo la necesidad de preservar la capacidad de los organismos de seguridad en Colombia. A continuación se indican las recomendaciones formuladas:

### I. Fortalecimiento de las capacidades institucionales de Ciberseguridad y Ciberdefensa

**- Se recomienda desarrollar una visión global ("la visión") para la Ciberseguridad**

De acuerdo con la misión de la OEA, el CONPES 3701 no aborda los problemas a un alto nivel, de forma que proporcione una visión estratégica clara, en la que se evidencie la comprensión actual del gobierno en el tema de Ciberseguridad – Ciberdefensa, y los objetivos generales, parecen no estar guiados por una visión estratégica para el país. En este sentido, los asuntos institucionales deben ser el resultado de la visión, y a su juicio esta visión debería contemplar:

[33] Estas recomendaciones fueron extraídas del documento: *"Misión de Asistencia Técnica en Seguridad Cibernética".* Conclusiones y Recomendaciones. OEA. Bogotá, 4 de abril de 2014. Puede consultarse en http://www.oas.org/documents/spa/press/Recomendaciones_COLOMBIA_SPA.pdf.

**Gráfico No. 6.** Visión global para ciberseguridad


Fuente: OEA. Misión de Asistencia Técnica en Seguridad Cibernética.2014

## II. Adoptar un enfoque global de la gestión de riesgos de ciberseguridad

El enfoque actual en Colombia tiene como objetivo preservar la seguridad en lugar de gestionar los riesgos, pero un enfoque basado en la gestión de riesgos permite obtener grandes beneficios de un entorno digital para lograr la prosperidad económica y social.
Por lo anterior se sugiere adoptar un enfoque global de la gestión de riesgos, que comprenda:

- ✓ La visión global de un enfoque de gestión de riesgos
- ✓ Establecer un programa nacional de gestión de riesgos[34]
- ✓ Realizar una evaluación integral de los riesgos de Ciberseguridad nacional

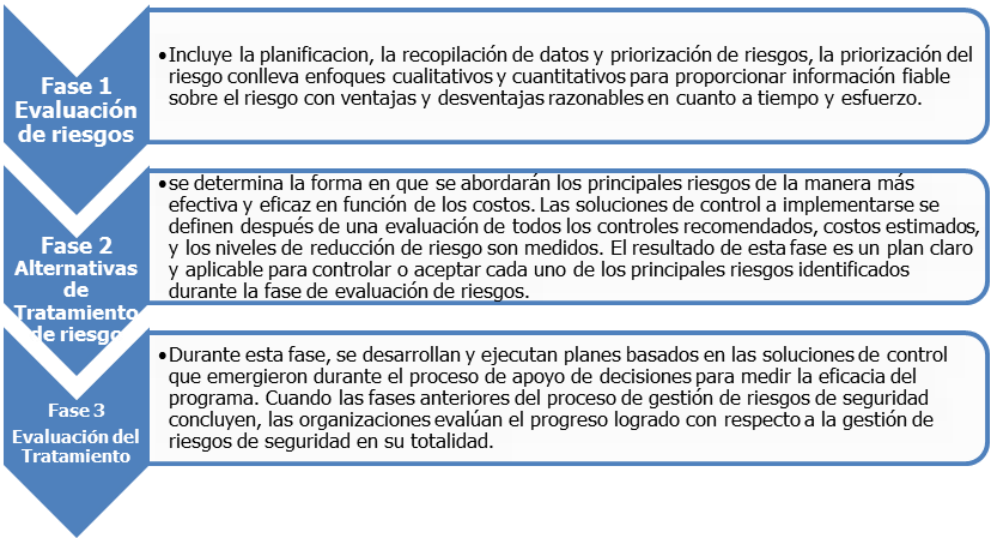
## III. Establecer un marco institucional claro y adoptar un sistema de gestión de riesgos cibernéticos adecuado

La OEA le recomienda a Colombia que establezca un órgano de coordinación permanente, que responda directamente al Presidente de la República y que el actual ColCERT se integre a este nuevo organismo coordinador, con el fin de asegurar que la política pública que se formule refleje un enfoque gubernamental coherente.

[34] Que incluya la evaluación, el tratamiento, la selección de medidas de seguridad, la preparación, la recuperación, y la metodología para que todos los actores evalúen y gestionen los riesgos de ciberseguridad, incluida la sensibilización, la formación etc.

Por otra parte, se sugiere que Colombia adopte un nuevo modelo de gestión de riesgos que incluya las fases descritas en el siguiente gráfico:

**Gráfico No. 7.** Modelo de Gestión de Riesgos




Fuente: Elaboración CRC a partir de OEA, Misión de Asistencia Técnica en Seguridad Cibernética

## IV. Establecer un proceso sistemático para involucrar a todos los interesados en el desarrollo de la estrategia y su implementación

El proceso sistemático deberá cumplir los cinco puntos relacionados en el siguiente gráfico:

**Gráfico No. 8.** Proceso Sistemático que involucre a todos los actores


Fuente: Misión de asistencia técnica en seguridad cibernética. OEA. 2014

## V. El Gobierno debe adoptar una política para la protección de la infraestructura crítica, teniendo en cuenta los aspectos de personal, físicos y lógicos

De acuerdo con la OEA, el enfoque del Gobierno Colombiano respecto a la definición y protección de la infraestructura crítica es bastante limitado, razón por la cual recomienda adoptar una política que gire en torno a los siguientes puntos:

**Gráfico No. 9.** Entorno seguridad infraestructura crítica

El aspecto digital (o ciber) de protección de la infraestructura crítica debe ser un subgrupo del enfoque global de la protección de la infraestructura crítica

La politica de infraestructura crítica contribuye a la prosperidad económica y social del país y a su defensa, por lo que la entidad de coordinación debe formular las politicas de protección.

Aunque la función del colCERT, contemplada en el CONPES 3701, refleja un enfoque apropiado, está función debería ubicarse como parte del organo de coordinación y no debería llamarse un "CERT".

Fuente: OEA. Misión de Asistencia Técnica en Seguridad Cibernética

## VI. Establecimiento y mejora de los marcos legales en Ciberseguridad[35]

1. Se recomienda de acuerdo con lo planteado por la REMJA[36] (OEA), que se reforme la legislación armonizándola con la Convención de Budapest, especialmente en materia de derecho procesal penal. Adicionalmente, se recomienda revisar legislaciones cibernéticas exitosas como la Ley 53-07 de República Dominicana[37] y la Ley 109/2009 del 15 de septiembre de Portugal. También, se recomienda tener en cuenta a la hora de redactar tipos penales, usar términos tecnológicamente neutrales para facilitar la interpretación de la Ley.
2. Adoptar medidas que prevén la responsabilidad de las personas jurídicas de acuerdo al artículo 12 de la Convención de Budapest.
3. La persecución de los delitos informáticos se debe separar de las cuestiones de ciberdefensa y ciberguerra, por lo que se debe definir cuál es la unidad policial que va a investigar y perseguir los delitos informáticos.
4. Establecer un régimen rápido y eficiente para asegurar la cooperación internacional en la prevención, investigación y persecución penal de los delitos informáticos, por lo que se recomienda específicamente establecer un punto de contacto para la Red 24/7, disponible las 24 horas del día los 7 días de la semana.
5. Crear en la fiscalía una unidad especializada para la investigación de los ciberdelitos.
6. Impartir capacitación a los jueces, fiscales y policías en materia de ciberdelitos, y en aspectos técnicos y jurídicos del tratamiento de la evidencia digital.
7. Implantar leyes con la participación del sector privado, para **regular** las obligaciones de las empresas que tienen **infraestructura critica**.
8. En el procedimiento para la investigación de delitos informáticos debe haber un balance entre eficiencia de la investigación y la **protección de garantías individuales** (intimidad – protección de datos).
9. Se recomienda adoptar medidas procesales para posibilitar la **preservación de la evidencia digital** (datos), de acuerdo a los artículos 16 y 17 de la Convención de Budapest.
10. Implementar legislativamente la **retención de datos de tráfico** por el término de 1 año (protección de datos personales).

---

[35] Para la adopción de estas recomendaciones es importante tener en cuenta la opinión del sistema penal, de la academia y de la sociedad civil.
[36] Grupo de expertos en delitos informáticos.
[37] Está Ley crea la Comisión Internacional contra crímenes y delitos de alta tecnología y crea el departamento de Investigación de crímenes y delitos de alta tecnología. La Ley 53-07 crea varias categorías de delitos como: los relacionados con el material de computadora (hardware), delitos relacionados con la privacidad, confidencialidad e integridad de los datos almacenados (incluye actos como el espionaje estatal, político, comercial, industrial), delitos de Telecomunicaciones (robo y reventa se señal de TV).

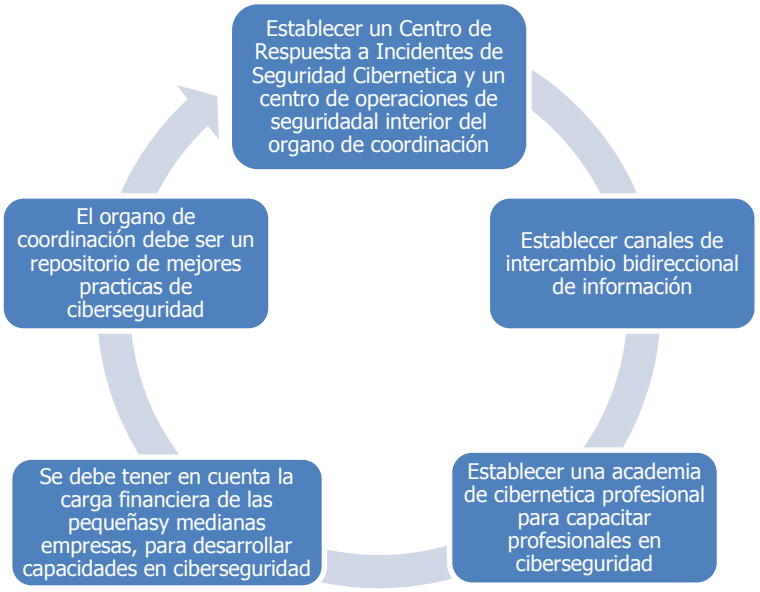
11. Solicitar a los gobiernos de las empresas proveedoras de servicios de internet, que tienen servidores con datos de ciudadanos Colombianos, que revisen los **mecanismos de cooperación en materia penal**, para que estas compañías respondan penalmente.

De las anteriores recomendaciones se observa como desde el sector TIC se puede apoyar en la definición de diferentes aspectos y principalmente los que están contemplados dentro de los numerales 7 a 11.

## VII. Generación de capacidades de Ciberseguridad y Ciberdefensa

En el siguiente gráfico se relacionan las cinco recomendaciones que deben ser atendidas para la generación de capacidades de Ciberseguridad y Ciberdefensa.

**Gráfico No. 10.** Recomendaciones Ciberseguridad y Ciberdefensa




Fuente: Misión de asistencia técnica en seguridad cibernética. OEA. 2014

### VIII. Cooperación internacional y cooperación entre múltiples partes interesadas

Para que la labor sea eficaz en materia de ciberseguridad, se requiere que todos los actores involucrados estén articulados y sean consultados, por lo que se recomienda, ente otros aspectos:

- ✓ Desarrollar una estrategia escrita para la cooperación internacional que aborde la ciberseguridad y el cibercrimen, donde se identifiquen prioridades, socios internacionales y objetivos.
- ✓ Fortalecer las funciones de la cancillería, en materia de cooperación internacional para la ciberseguridad.
- ✓ Crear la posición de coordinador de la política cibernética internacional, cuya tarea principal será la implementación de la estrategia de cooperación internacional.
- ✓ Establecer un mecanismo de cooperación formal entre el gobierno y el sector privado, que sea seguro para el intercambio de información de incidentes de ciberseguridad nacional e internacional.
- ✓ Implantar un plan de capacitación internacional apoyado por los altos niveles del gobierno para disminuir la brecha del conocimiento.[38]
- ✓ Facilitar el intercambio de datos con respecto a incidentes de ciberseguridad *(International Watch and Warning Network, Forum for Incident Response).*
- ✓ Colombia deberá adherir al sistema I-24/7 de INTERPOL para todas las unidades de las fuerzas de seguridad del cibercrimen en Colombia.
- ✓ Fortalecer el conocimiento académico en ciberseguridad.
- ✓ Establecer un marco para facilitar el intercambio directo de información entre equipos de respuesta e incidentes cibernéticos de otros países.
- ✓ Asegurarse que todas las actividades internacionales que involucren el intercambio de datos personales respeten las leyes internacionales de derechos humanos (derecho a la privacidad).

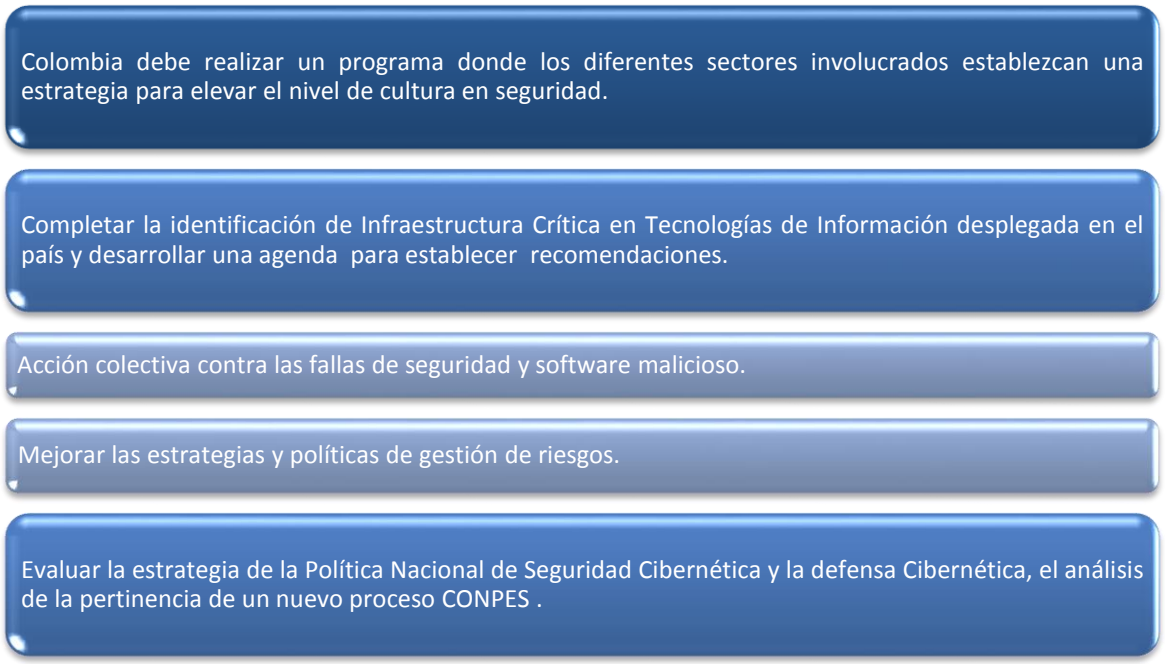
## 4.5 RECOMENDACIONES DE LA OECD

Colombia ha implantado en los últimos años medidas acertadas como es la creación de la Dirección de Seguridad Pública y de Infraestructura del Ministerio de Defensa Nacional, y la creación del ColCERT, que son organismos encargados de la formulación y ejecución de planes y programas, en materia de Ciberdefensa de la infraestructura critica nacional.

[38] El plan de formación deberá incluir las necesidades de los funcionarios de todas las áreas del gobierno involucradas en la ciberseguridad y el cibercrimen, así como fiscales, jueces y demás funcionarios que apliquen la Ley.

No obstante, la OECD ha realizado algunas recomendaciones dentro del estudio adelantado sobre políticas y regulación en telecomunicaciones de Ciberseguridad para que sean aplicadas por Colombia[39], en el Gráfico No. 11 se enmarcan algunas de las recomendaciones más relevantes las cuales están siendo tenidas en cuenta por las diferentes Entidades del Gobierno para incorporarlas en la definición de una nueva estrategia de Ciberseguridad y Ciberdefensa para el país.

**Gráfico No. 11** Recomendaciones OECD




Fuente: Elaboración CRC a partir de información OCDE

De lo anterior se observa que es importante incorporar en la nueva estrategia, medidas puntuales respecto a la definición y protección de la infraestructura crítica nacional, así como adoptar un nuevo esquema de riesgos para eventos de ataques cibernéticos, adicionalmente se debe hacer un seguimiento a la serie de instrumentos generales que presenta la OECD[40] tales como guía, recomendaciones generales, resultados de mesas de trabajo y toda documentación que pueda ser acogida por los países miembros, las cuales deberán ser analizadas y de ser pertinente, acogidas por

[39] Fuente: MinTIC y OCDE, http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=121&InstrumentPID=117&Lang=en&Book,
[40] http://webnet.oecd.org/OECDACTS/Instruments/ListBySubjectView.aspx)

Colombia durante el proceso de adhesión a la OECD, teniendo en cuenta también que en el mes de enero del 2015 se adelantó la revisión de las directrices de seguridad cibernética lo que significa que Colombia tendrá que cumplir con la nueva versión de las recomendaciones adoptadas y definir una agenda de trabajo que permitan definir responsabilidades y responsables para el cumplimiento de las mismas.

De otro lado, la Recomendación del Consejo de la OCDE sobre la protección de infraestructuras críticas[41] de información adoptada en abril de 2008 [C (2008) 35][42] se entiende la relevancia de las Directrices de Seguridad de la OCDE a la CII en la cual se proporciona orientación sobre las políticas nacionales y propone formas de mejorar la cooperación internacional para la protección de la CII, dicha orientación se deriva de las mejores prácticas identificadas en un estudio comparativo de la OCDE sobre políticas de la CII en siete países.

La Recomendación señala la necesidad de fortalecer la cooperación internacional para hacer frente a las cuestiones transfronterizas, dada la importancia de Internet como una infraestructura global. También identifica la necesidad de una capacidad nacional de seguridad de la infraestructura operativa, la voluntad y la capacidad de compartir información, una estrecha cooperación con las partes pertinentes del sector privado, y una sólida cultura de la seguridad en la cara de un rápido crecimiento tecnológico y los cambios sociales consecuentes. Por ello, la Recomendación establece un enfoque común en una serie de áreas que permita avanzar en algunos de estos temas. Además, aunque la Recomendación se dirige a los gobiernos, hace hincapié en la necesidad de colaboración con el sector privado.

La Recomendación consta de dos partes:

1) La protección de infraestructuras críticas de información a nivel nacional. Los países miembros deben:

- Demostrar liderazgo del gobierno y el compromiso de proteger CII
- Administrar los riesgos para la CII
- Trabajar en asociación con el sector privado

[41] La expresión "infraestructura crítica" se aplica a sectores o servicios que son críticos para la seguridad y la protección de la sociedad, la economía y el gobierno, tales como el transporte o la energía. Las "infraestructuras críticas de información" (CII) se ha convertido en la comunidad internacional como un término neutro y general para referirse a las redes y sistemas de información.

[42] OECD, 2008. c(2008)35 *Draft recommendation of the council on the protection of critical information infrastructures.* Extraído de www.oecd.org

2) La protección de infraestructuras críticas de información a través de fronteras. Los países miembros deben:

- Cooperar entre ellos y con el sector privado en la estrategia, la política y los niveles operativos para garantizar la protección de la CII contra eventos y circunstancias más allá de la capacidad de cada país para hacer frente por sí solo
- En particular, participar en la cooperación bilateral y multilateral en los ámbitos regional y mundial
- Apoyo a la colaboración transfronteriza, y el intercambio de información sobre investigación y desarrollo público-privada para la protección de la CII

El pasado mes de junio de 2015, la Dirección de Ciencia Tecnología e Innovación de la OCDE, publicó el *"Proyecto de recomendación del Consejo sobre la gestión de riesgos de seguridad digital para la prosperidad económica y social"*, en el cual se establece una serie de principios que pretenden complementar los procesos de gestión de riesgos de seguridad digital.

En el mencionado proyecto se define el *"riesgo de seguridad digital"*[43] como una categoría del riesgo relacionado con el uso, desarrollo y gestión de lo digital en el desarrollo de cualquier actividad. Este riesgo puede ser el resultado de la combinación de amenazas y vulnerabilidades en el entorno digital, este riesgo puede vulnerar el ejercicio de los derechos económicos y sociales, afectando la confidencialidad, la integridad y disponibilidad de las actividades que se desarrollen en el entorno digital.

Por otra parte, el proyecto define la *"gestión de riesgos de seguridad digital"* como el conjunto de acciones coordinadas abordadas en una organización para hacer frente a los riesgos de seguridad digital maximizando las oportunidades. La gestión de riesgos de seguridad digital comprende un conjunto integral, sistemático y flexible de procesos cíclicos, que aseguran que se adopten "medidas de seguridad" apropiadas y acordes con el riesgo y los objetivos económicos y sociales en juego.

Adicionalmente, el documento determina que las *"partes interesadas"* son los gobiernos, las organizaciones públicas y privadas, los individuos que desarrollan en el entorno digital la totalidad o parte de sus actividades económicas y sociales.

[43] Es importante mencionar que la OCDE considera que el riesgo de seguridad digital es de naturaleza dinámica, puesto que incluye o envuelve aspectos relacionados con lo digital y los entornos físicos, involucra también a las personas y organizaciones que desarrollan actividades en el entorno digital.

Así mismo, el Proyecto de recomendaciones consagra los siguientes principios generales:

1. Conocimiento, habilidades y empoderamiento. *"Todas las partes interesadas deben entender los riesgos de seguridad digital y cómo manejarlos"*

Las partes involucradas deben ser conscientes que el riesgo de seguridad digital puede afectar la consecución de sus objetivos económicos y sociales, y que adicionalmente la gestión de su propio riesgo de seguridad digital puede afectar a otros. De esta manera, las partes involucradas deberían contar con la educación y las habilidades necesarias para gestionar este tipo de riesgo y para evaluar el posible impacto de sus decisiones de gestión de riesgos de seguridad digital en sus actividades y el entorno digital en general.

2. Responsabilidad. *"Todas las partes interesadas deben asumir la responsabilidad de la gestión de riesgo de seguridad digital"*

Las partes interesadas deben actuar con responsabilidad y rendir cuentas, sobre la base de sus funciones, el contexto y su capacidad para actuar, para la gestión del riesgo de seguridad digital y para tener en cuenta el posible impacto de sus decisiones sobre los demás. Adicionalmente, deben reconocer que un cierto nivel de riesgo de seguridad digital tiene que ser aceptado para lograr los objetivos económicos y sociales.

3. Los derechos humanos y los valores fundamentales. *"Todos los interesados deben gestionar el riesgo de seguridad digital de manera transparente y coherente con los derechos humanos y los valores fundamentales"*

- La gestión de riesgos de seguridad digital se debe manejar de una manera consistente con los derechos humanos y los valores fundamentales reconocidos por las sociedades democráticas, incluida la libertad de expresión, el libre flujo de información, la confidencialidad de la información y la comunicación, la protección de la privacidad y los datos personales, la transparencia y el debido proceso.

- La gestión de riesgos de seguridad digital debe basarse en la conducta ética que respeta y reconoce los intereses legítimos de los demás y de la sociedad en su conjunto.

- Las organizaciones deben tener una política general de transparencia acerca de sus prácticas y procedimientos para la gestión de riesgos de seguridad digital.

4. Cooperación. *"Todas las partes interesadas deberían cooperar, incluso a través de las fronteras"*

La interrelación mundial crea interdependencias entre las partes interesadas y las llamadas por su cooperación en la gestión de riesgos de seguridad digital. De esta manera, debe existir cooperación entre los gobiernos, las organizaciones públicas y privadas, y la sociedad civil. Adicionalmente, la cooperación debe darse a través de las fronteras regionales e internacionales.

Por otra parte, el Proyecto de recomendaciones consagra los siguientes principios operacionales:

1. La evaluación de riesgos y el ciclo de tratamiento. *"Los líderes y los actores que toman decisiones deben asegurarse de realizar una evaluación continua del riesgo"*

- La evaluación de riesgos de seguridad digital debe llevarse a cabo como un proceso sistemático y cíclico en curso. Por lo cual, se deben evaluar las posibles consecuencias de las amenazas combinadas con vulnerabilidades en las actividades sociales económicas en juego.

- El tratamiento del riesgo debería tener como objetivo reducir el riesgo a un nivel aceptable para los beneficios económicos y sociales que se esperan de las actividades teniendo en cuenta el impacto potencial sobre los intereses de los demás.

- El tratamiento del riesgo incluye varias opciones: aceptar el riesgo, reducirlo, transferirlo, evitarlo o una combinación de ellos.

2. Las medidas de seguridad. *"Los líderes y los actores que toman decisiones deben asegurarse de que las medidas de seguridad son apropiadas y que corresponden al riesgo"*

- La evaluación del riesgo de seguridad digital, debe guiar la selección, operación y mejora de las medidas de seguridad para reducir el riesgo hasta un nivel aceptable.

- Las medidas de seguridad deben ser apropiadas y proporcionales al riesgo y en su selección se deben tener en cuenta su impacto potencial negativo y positivo en las actividades económicas y sociales que tienen por objeto proteger los derechos humanos y los valores fundamentales y los intereses legítimos de los demás. Todos los tipos de medidas deben ser considerados, ya sean físicas, digitales, o relacionadas con personas, procesos o tecnologías involucradas en las actividades.

- Las organizaciones deben buscar y tratar adecuadamente las vulnerabilidades tan pronto como sea posible.

3. Innovación

La innovación debe ser considerada como parte integral de la reducción del riesgo de seguridad digital hasta un nivel aceptable, por lo cual la innovación se debe tener en cuenta al momento de determinar la evaluación y tratamiento de riesgos. La innovación debe fomentarse tanto en el diseño y operación de las actividades económicas y sociales que dependen de un entorno digital, así como en el diseño y desarrollo de medidas de seguridad.

*4.* Preparación y continuidad. "*Los líderes y los actores que toman decisiones deben garantizar que se adopte un plan de preparación y continuidad"*

- Los líderes y los actores que toman decisiones en la evaluación de riesgos de seguridad digital, deben adoptar un plan de preparación y continuidad con el fin de reducir los efectos adversos de los incidentes de seguridad, y apoyar la continuidad y la capacidad de recuperación de las actividades económicas y sociales.

- El plan debe identificar las medidas para prevenir, detectar, responder y recuperarse de incidentes de seguridad digital. Adicionalmente, debe proporcionar mecanismos para atribuir niveles claros de escalamiento basado en la magnitud y gravedad de los efectos de los incidentes de seguridad digitales, así como su potencial para extender a los demás en el entorno digital.

- Se deben incluir procedimientos de notificación apropiados para ser considerados como parte de la implementación del plan.

El proyecto de recomendaciones establece que las estrategias nacionales para la gestión de riesgos de seguridad digital deben ser coherentes con los principios expuestos (generales y operacionales), con el fin de que surjan las condiciones adecuadas para que todas las partes interesadas desarrollen con confianza actividades económicas y sociales en el entorno digital. De esta manera, las estrategias nacionales deberían atender las siguientes recomendaciones:

- Que desde el nivel más alto del gobierno nacional se formule un enfoque claro, flexible, tecnológicamente neutral y coherente con otras estrategias de promoción de la prosperidad económica y social.

- Se debe aprovechar el entorno digital, reduciendo el nivel general de riesgo de seguridad digital, al interior del país y en las fronteras, sin reducir el flujo de las tecnologías, las comunicaciones y los datos.

- La estrategia se debe dirigir a todos los actores interesados[44], y así mismo se debe articular la responsabilidad y la rendición de cuentas de los interesados de acuerdo con sus funciones, capacidad de actuar y el contexto en el que operan.

Finalmente, el proyecto de acuerdo establece que las estrategias nacionales deben incluir las siguientes medidas:

- Adoptar un marco integral para la gestión de riesgos de seguridad digital para las actividades propias del gobierno.
- Establecer mecanismos de coordinación entre todos los actores gubernamentales pertinentes, para garantizar que su gestión del riesgo de seguridad digital es compatible y mejora la economía.
- Establecer uno o más equipos de respuesta a incidentes de seguridad informática (CSIRT).
- Se debe fomentar la gestión de riesgos de seguridad digital en toda la economía.
- Se deben adoptar técnicas de seguridad innovadoras para la gestión de riesgos de seguridad digital, con el fin de proteger efectivamente la información y los datos (almacenados o en tránsito).
- Apoyar el desarrollo de una fuerza laboral capacitada que pueda mejorar el riesgo de seguridad digital.
- Adoptar e implementar un marco legal integral que mitigue la delincuencia informática.
- Asegurar que se asignen los recursos suficientes para aplicar eficazmente la estrategia.
- Fortalecer la cooperación internacional y la asistencia mutua.
- Generar las condiciones adecuadas para que todos los actores interesados colaboren y aporten en la gestión de la seguridad digital.

[44] Incluyendo a las medianas y pequeñas empresas y a las personas.

### 4.6 Unión Internacional de Telecomunicaciones (UIT)

En el año 2007 la Secretaría General de la UIT lanzó la Agenda de Ciberseguridad Global (GCA, por sus siglas en inglés), que consiste en un marco para la cooperación internacional cuyo propósito es mejorar la seguridad y la confiabilidad en la sociedad de la información. La GCA está diseñada con el fin de facilitar la cooperación entre los participantes y de esta forma construir propuestas que contribuyan a contrarrestar ciberataques, evitando la duplicación de esfuerzos[45].

La GCA se construye sobre cinco pilares estratégicos, también conocidos como áreas de trabajo:

I. **Medidas Legales**: Estrategias para diseñar una legislación modelo sobre el ciberdelito que es compatible y aplicable mundialmente.
II. **Medidas técnicas y procedimentales**: Propuestas encaminadas a establecer un marco de diálogo, cooperación y coordinación internacionales.
III. **Estructuras organizacionales**: Estrategias mundiales tendientes a establecer estructuras institucionales y políticas sobre ciberdelito, vigilancia, alerta y respuesta ante incidentes y un sistema de identidad digital genérica y universal.
IV. **Fortalecimiento de capacidades**: Objetivos estratégicos para facilitar la constitución de capacidad humana e institucional.
V. **Cooperación Internacional**: Propuestas encaminadas a establecer un marco de diálogo, cooperación y coordinación internacional.

En el marco de actividades de esta Agenda, se realizó en 2014 la medición del Global Cibersecurity Index[46], el cual ya ha sido mencionado en el aparte de antecedentes del presente documento el cual ubica a Colombia en la posición No.9[47] cerca de países tan importantes en la aplicación de buenas prácticas sobre Ciberseguridad como Israel, el cual ha sido denominado como el país *"Startup Nation"* o también *"Innovation Nation"* debido a su alto grado de innovación y de preparación en estos temas a nivel mundial; es así como Colombia ha recibido el reconocimiento a los esfuerzos adelantados en para contrarrestar las crecientes amenazas en temas del ciberespacio.

[45] Consultado en el enlace: http://www.itu.int/osg/csd/cybersecurity/gca/
[46] El GCI nace de una asociación de cooperación entre el sector privado y la organización internacional para impulsar el tema de la seguridad cibernética a la vanguardia de las agendas nacionales. El proyecto es el resultado de la investigación primaria y secundaria intensiva por la UIT y ABI Research. A la fecha, 103 países respondieron al GCI.
[47] http://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI_Global_2014_results.pdf

Ahora bien, en términos de estandarización, el objetivo de la UIT es buscar un trabajo coordinando entre el sector público y privado, con el fin de armonizar las políticas y estándares de seguridad a nivel internacional.

La UIT ha desarrollado tanto Recomendaciones, como una visión general de los requisitos y directrices de seguridad aplicables a protocolos. Las especificaciones de seguridad en sistemas IP definen como identificar ciberamenazas y contrarrestarlas para mitigar los riesgos. El trabajo en comunicaciones seguras revisa mejoras a las especificaciones de seguridad para comunicaciones de datos extremo a extremo y considera requerimientos de seguridad para servicios web y protocolos de capa de aplicación.

La Recomendación UIT-T X.1205 "Aspectos Generales de la Ciberseguridad" ofrece una definición de ciberseguridad. En ella se expone la clasificación de las amenazas de seguridad desde el punto de vista de una organización. Se presentan las amenazas a la ciberseguridad, así como sus puntos débiles, incluidas las herramientas más utilizadas por los piratas informáticos. Se tratan las amenazas en las distintas capas de red. Se exponen también diversas tecnologías de ciberseguridad disponibles para contrarrestar las amenazas, como pueden ser los enrutadores, firewall, antivirus, sistemas de detección de intrusión, sistemas de protección de intrusos, la computación segura y la auditoría y supervisión. Se exponen los principios de protección de la red, como la defensa en profundidad y la gestión de acceso aplicadas a la ciberseguridad. También trata las estrategias y técnicas de gestión de riesgos, incluido la importancia de la formación y la educación a la hora de proteger la red. Así mismo presenta ejemplos de cómo se protegen diversas redes con las tecnologías presentadas.

Por su parte, la Recomendación UIT-T X.805 define la arquitectura de seguridad para sistemas que proveen comunicaciones extremo a extremo. Esta recomendación permite a los operadores determinar con precisión los puntos vulnerables en una red para darles un adecuado tratamiento.

La Recomendación UIT-T X.509[48] fue desarrollada con el fin de proveer mecanismos de autenticación electrónica sobre redes públicas, a través del uso de certificados de llaves públicas y el diseño de aplicaciones relacionadas con infraestructura de llave pública. Se utiliza para asegurar conexiones entre navegadores web y servidores con el fin de proteger la información que se intercambia, así mismo protege las transacciones que se realicen por comercio electrónico, para determinar la autenticidad de información proveniente de correos electrónicos, uso de firmas y certificados digitales.

[48] http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509

A nivel más específico, por ejemplo las series UIT-T H.235.x definen la seguridad de infraestructura y servicios (incluyendo autenticación y privacidad) para el uso de sistemas H.300 (como es el caso de servicios de videoconferencia y VOIP que usan el protocolo H.323). Por su parte, para los sistemas de Televisión que hacen uso de arquitectura IPCablecom, la especificación de seguridad UIT-T J.170 define los requerimientos de seguridad para entregar servicios seguros incluyendo el de VoIP.

Por otro lado, el Grupo de Estudio 17 (SG17) trabaja con el objetivo de crear seguridad y confiabilidad en el uso de TIC y ha publicado más de setenta estándares (Recomendaciones ITU-T) enfocados en temas de seguridad. El SG17 coordina todo el trabajo que esté relacionado con temas de seguridad a través de todos los grupos de estudio de la UIT-T.

Dentro del SG17, el C4 estudia los métodos para determinar en tiempo real la integridad de la seguridad de los servicios y sistemas y recopilar y mantener datos de incidentes de seguridad relevantes.

Entre otros temas, el SG17 trabaja en ciberseguridad; gestión de seguridad, marcos de referencia y arquitecturas de seguridad, lucha contra el spam, gestión de identidad, la protección de información personal, y la seguridad de aplicaciones y servicios para el Internet de las cosas (IoT), redes inteligentes, smartphones, web services, redes sociales, cloud computing, sistemas financieros móviles, IPTV y telebiométricos.

La Comisión de Estudio 17 de la UIT-T está actualmente elaborando normas en las siguientes áreas:

- C 1/17 Coordinación de la seguridad de las telecomunicaciones / TIC
- C 2/17 Arquitectura y marco de seguridad
- C 3/17 Gestión de seguridad informática de las telecomunicaciones
- C 4/17 Ciberseguridad
- C 5/17 Combatir el correo basura (spam) a través de medios técnicos
- C 6/17 Asegurar aspectos de los servicios de telecomunicaciones ubicuos
- C 7/17 Asegurar los servicios de aplicación
- C 8/17 Seguridad de la computación en nube
- C 9/17 Telebiometría
- C 10/17 Arquitectura y mecanismos de la gestión de identidad
- C 11/17 Tecnologías genéricas en apoyo de las aplicaciones seguras

## 4.7 Otros organismos internacionales

### 4.7.1 ETSI

El Instituto de Estandarización de Telecomunicaciones Europeo hace algunos años publicó una Guía para Diseño de Seguridad para la aplicación de Criterios Comunes[49] en los entregables de ETSI. Este trabajo se desarrolla dentro de dos grupos: End to End Network Architectures (E2NA) y Technical Committee Network Technologies (NTECH).

Adicionalmente cuenta con un Grupo de Expertos en Algoritmos de Seguridad que desarrolla algoritmos de seguridad y encripción para uso en las tecnologías estandarizadas de ETSI, el Comité de Plataformas de Tarjetas Inteligentes desarrolla estándares utilizados para asegurar las comunicaciones y las redes móviles que usan Sim Card. [50]

En el año 2011 se estableció el Grupo de Coordinación de Ciberseguridad de CEN-CENELEC y ETSI (CSCG, por sus siglas en inglés). El grupo CSCG asesora los grupos técnicos de CEN, CENELEC y ETSI en asuntos estratégicos relacionados con seguridad IT, redes y seguridad de la información (NIS) y ciberseguridad. El CSCG trabaja muy de cerca con aliados internacionales (principalmente en Estados Unidos), con instituciones de la Unión Europa (incluyendo la Agencia de la Unión Europea para las Redes y la Seguridad de la Información), y con organizaciones internacionales de estandarización (ISO e IEC)

Específicamente en Febrero de 2013 se publicó el documento *"Estrategia de Ciberseguridad en la Unión Europea: Un Ciberespecio Abierto, Seguro y Protegido".* La estrategia articula la visión de ciberseguridad de la Unión Europea en términos de cinco prioridades: alcanzar ciber resilencia, reducir drásticamente el cibercrimen, desarrollar políticas de ciberdefensa, desarrollar los recursos industriales y tecnológicos para la ciberseguridad y establecer una política de ciberespacio internacional coherente para la Unión Europea. [51]

Adicionalmente ETSI decidió establecer un nuevo Comité Técnico (TC CYBER) con el fin de desarrollar estándares relacionados específicamente con Ciberseguridad. La primera reunión se llevó a cabo en

[49] Los Criterios Comunes(CC) tienen su origen en 1990 y surgen como resultado de la armonización de los criterios sobre seguridad de productos software ya utilizados por diferentes países con el fin de que el resultado del proceso de evaluación pudiese ser aceptado en múltiples países.
[50] http://www.etsi.org/news-events/news/769-2014-03-etsi-to-develop-european-standards-for-cybersecurity
[51] http://www.etsi.org/news-events/news/773-2014-04-press-release-european-standardization-organizations-discuss

mayo de 2014 y el propósito es manejar las crecientes demandas de estandarización en las siguientes áreas[52]:

- Ciberseguridad
- Seguridad infraestructuras, equipos, servicios y protocolos
- Recomendaciones de seguridad, guía y requerimientos de seguridad operacional para usuarios, fabricantes y operadores de infraestructuras y redes.
- Herramientas y técnicas para mejorar la seguridad
- Creación de especificaciones de seguridad y alineación con el trabajo realizado por otros comités de ETSI.

### 4.7.2 3GPP

El 3GPP (3rd Generation Partnership Project) es el cuerpo principal de estándares globales para servicios y redes móviles. Dentro de los cuatro Grupos de Especificaciones Técnicas (TSG, por sus siglas en inglés), Aspectos de Servicio y Sistemas (SA) y Terminales y Red Core (CT) se enfocan en garantía de seguridad.

Dentro del Grupo de Aspectos de Servicio y Sistemas (WG SA3) se ha iniciado un trabajo para elaborar un esquema que garantice que los elementos de red se desarrollen de manera segura y que los niveles de seguridad puedan evaluarse.

### 4.7.3 IEEE

La asociación de estándares IEEE es un organismo privado que está formado por varios comités independientes de estándares. Dentro de esta organización se creó el Grupo de Seguridad en Conexiones de la Industria (ICSG, por sus siglas en inglés), del cual hacen parte entidades que trabajan en seguridad informática, quienes aportan su experiencia y recursos para combatir las crecientes y cada vez más sofisticadas amenazas informáticas. Específicamente el Grupo de Trabajo de Seguridad de Malware está desarrollando estándares para el intercambio de meta data de malware, con el fin de responder de forma más eficiente y efectiva a las amenazas que se realizan a través del uso de este tipo de software[53].

Otros estándares que tratan temas relacionados con ciberseguridad son:

[52] http://www.etsi.org/news-events/news/769-2014-03-etsi-to-develop-european-standards-for-cybersecurity
[53] http://standards.ieee.org/develop/indconn/icsg/index.html

- IEEE 802.10. El 802.10 fue un estándar definido para seguridad en redes LAN/MAN con el fin de tratar los problemas que se presentaban al interoperar este tipo de redes. Estas recomendaciones incluían autenticación, control de acceso, integridad de datos y confidencialidad. En 2004 sus especificaciones fueron contenidas en especificaciones como 802.11 (implementación de capas física y de acceso de redes WLAN) y 802.1q (estándar para uso de VLAN)
- IEEE P1619 (Security in Storage Working Group): corresponde a una familia de estándares para la protección de datos almacenados y el manejo de llaves criptográficas para dicha protección. Incluye modos específicos de uso de llaves y algoritmos de cifrado.
- IEEE 2600 Hardcopy Device and System Security: Este estándar define los requerimientos de seguridad para fabricantes y usuarios en la selección, instalación configuración y uso de dispositivos y sistemas de impresión, incluyendo impresoras, copiadoras y equipos multifuncionales.

### 4.7.4 ICANN

El Comité Asesor de Seguridad y Estabilidad o SSAC[54] de sus siglas en inglés (Security and Stability Advisory Committee) asesora a la comunidad de ICANN y a la Junta en relación a i) asuntos con la seguridad e integridad de los sistemas en la asignación de nombres y direcciones de Internet, incluyendo asuntos como el funcionamiento correcto y fiable del sistema de nombres de la raíz, ii) cuestiones administrativas como los relativos a abordar la asignación de números de Internet, iii) y las cuestiones de registro como los relativos al registro de servicios como WHOIS[55]. El SSAC se involucra en análisis de evaluación de amenazas y riesgos en curso de los servicios de nombres de Internet y de asignación de direcciones para evaluar las principales amenazas para la estabilidad y seguridad.

Ahora bien, dentro de la estructura de trabajo de ICANN también se cuenta con un equipo dedicado a seguridad, estabilidad y resiliencia (SSR) en la red de Internet, la cual contribuye con establecer recomendaciones generales, para contrarrestar amenazas de seguridad, es así como ha emitido reportes y análisis para contrarrestar los ataques originados de DDoS a través de los DNS[56] los cuales cada vez tienen un mayor incremento y frecuencia.

---

[54] https://www.icann.org/groups/ssac
[55] WHOIS es un protocolo TCP basado en petición/respuesta que se utiliza para efectuar consultas en una base de datos
[56] El DNS está compuesto por una cadena de queries enviados desde el navegador del usuario hasta un servidor que tiene la autoridad para responder. Simplificando el proceso, si usted quiere visitar 'ejemplo.com', su navegador enviará un query a un

Dentro de las recomendaciones hechas se encuentra la implementación del BCP[57] 38, la cual "*describe la solución a esta vulnerabilidad (o una defensa, depende de a quién se pregunte): que todos los proveedores de servicios de Internet implementen una técnica denominada Source Address Validation. Si un ISP ha implementado el BCP 38, al recibir un paquete IP que diga venir de una dirección IP por fuera de los rangos de IPs que le hayan sido asignados, su servidor lo bloqueará y no lo dejará pasar"*[58].

De otro lado, de acuerdo con ICANN, se han detectado vulnerabilidades en el DNS que permiten que un atacante fuerce el proceso de buscar una persona o buscar un sitio en Internet utilizando su nombre. El objetivo del ataque es tomar el control de la sesión para, por ejemplo, enviar al usuario al propio sitio web fraudulento del atacante, con el fin de obtener los datos de la cuenta y la contraseña.

Estas vulnerabilidades han aumentado el interés por introducir una tecnología denominada Extensiones de seguridad del DNS o DNSSEC[59] por su sigla en inglés para proteger este aspecto de la infraestructura de Internet, mediante la firma digital de clave pública (PKI, la sigla en inglés) de los datos a fin de tener la seguridad de que son válidos. Sin embargo, para eliminar esta vulnerabilidad de Internet, esta tecnología se debe implementar en cada uno de los pasos del proceso de búsqueda, desde la zona raíz hasta el nombre de dominio final.

Los diferentes procesos de análisis de vulnerabilidades, estrategias para su mitigación y seguimiento a medidas adoptadas, son adelantados de manera permanente por los diferentes integrantes dentro del modelo multi *stake holder* de ICANN.

## 5. EXPERIENCIAS INTERNACIONALES EN CIBERSEGURIDAD

### 5.1 Unión Europea (UE)

En el año 2013 la Comisión Europea publicó el documento titulado "Estrategia de Ciberseguridad de la Unión Europea: Un Ciberespacio abierto, seguro y protegido"[60], que aborda de manera general el

---

servidor de DNS preguntándole la dirección IP en la que 'ejemplo.com' está alojado. El servidor de DNS buscará la respuesta al query y la enviará de vuelta.

[57] Best Current Practice

[58] Consultado en: https://www.icann.org/news/blog/ataques-ddos-amplificados-la-mas-grande-amenaza-contra-internet, BCP38 http://tools.ietf.org/html/bcp38

[59] https://www.icann.org/resources/pages/dnssec-qaa-2014-01-29-es

[60] Propuestas y antecedentes: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security
Documento Final: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667

problema de la Ciberseguridad, con el objetivo de garantizar la seguridad en la prestación de los servicios TIC, así como dar cumplimiento a los Derechos y Valores fundamentales de la UE en esta materia.

El documento identifica en cada capítulo tareas para los órganos de la UE, ENISA, los estados miembros y la industria, señalando 5 estrategias prioritarias:

- La resiliencia contra los ataques
- La reducción drástica de la delincuencia en la red
- El desarrollo de una política de ciberdefensa y de las capacidades correspondientes en el ámbito de la Política Común de Seguridad y Defensa (PCSD)
- El desarrollo de los recursos industriales y tecnológicos necesarios en materia de ciberseguridad
- El establecimiento de una política internacional coherente del ciberespacio en la UE y la promoción de los valores Europeos esenciales.

En el caso del plan presentado por la Unión Europea destaca la solicitud a los estados miembros designar autoridades que se encarguen de la seguridad de los sistemas de información, y que a través de los Equipos de Respuesta a Incidentes de Seguridad de la Información (CERT) permitan mantener y restaurar la operatividad sus redes y sistemas de información.

Otro punto que cabe destacar del plan europeo es orientar a los estados miembros hacia la adopción de prácticas para la gestión de riesgos en las administraciones públicas y para los operadores de servicios financieros, de transportes, servicios de energía y para los prestadores de servicios que operen con información sensible de los usuarios, como son los servicios de pagos y comercio electrónico, servicios de computación en la nube o redes sociales.

Por otra parte, la propuesta de Directiva[61] del Parlamento Europeo y del Consejo sobre "Seguridad de la Información y Redes (SRI)" fue aprobada en febrero de 2014, y define tres líneas prioritarias de acción:

1. Imponer a todos los Estados miembros la obligación de velar por que exista un nivel mínimo de capacidades nacionales mediante la designación de autoridades competentes en materia de SRI, la creación de equipos de respuesta a emergencias informáticas (CERT) y la adopción de estrategias y planes de cooperación nacionales en el ámbito de la SRI.

[61] Puede ser consultada en el link: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:ES:PDF

2. Las autoridades nacionales competentes deberán cooperar dentro de una red que garantice una coordinación segura y eficaz y, en particular, un intercambio coordinado de información y unas labores de detección y respuesta a escala de la UE. A través de esta red, los Estados miembros deberán intercambiar información y cooperar para hacer frente a las amenazas e incidentes que puedan poner en peligro la SRI sobre la base del plan de cooperación europeo en materia de SRI.
3. Implantar una cultura de gestión de riesgos y garantizar el intercambio de información entre los sectores público y privado. Las empresas de los sectores críticos concretos antes citados y las administraciones públicas deberán evaluar los riesgos a que se enfrentan y adoptar medidas adecuadas y proporcionadas para garantizar la SRI. Estas empresas deberán notificar a las autoridades competentes todos los incidentes que supongan un peligro grave para el funcionamiento de sus redes y sistemas de información y comprometan de forma significativa la continuidad de los servicios críticos y el suministro de mercancías.

Adicionalmente la UE ha adoptado medidas adicionales como el European Public – Private Partnership for Resilience (EP3R): Fue creada con el fin de apoyar la coordinación y el programa de Critical Information Infrastructure Protection (CIIP)[62]; los objetivos de EP3R son cuatro:

- Fomentar el intercambio de información y el crecimiento de valores de buenas políticas y prácticas industriales para fomentar el entendimiento común;
- Discutir las prioridades de política pública, objetivos y medidas;
- Requisitos de referencia para la seguridad y resiliencia en Europa ;
- Identificar y promover la adopción de buenas prácticas elementales de seguridad y resiliencia.

De otra parte, en abril de 2014 el Tribunal de Justicia Europeo declaró inválida la Directiva 2006/24/CE del Parlamento y Consejo Europeo, *"sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones".*

Así, la Directiva establecía que los proveedores debían conservar los datos de tráfico y de localización, así como los datos necesarios para identificar al abonado o al usuario, sin embargo la Directiva no autorizaba la conservación del contenido (de las conversaciones telefónicas o de los correos electrónicos). El Tribunal de Justicia consideró en la sentencia que declara invalida la Directiva 2006/24/CE, que los datos que se conservan, permiten saber con qué persona y de qué modo se ha

[62] http://www.enisa.europa.eu/activities/Resilience-and-CIIP

comunicado un abonado o un usuario registrado, además de determinar el momento de la comunicación y el lugar desde que esta se ha producido y conocer la frecuencia de las comunicaciones del abonado o del usuario registrado con determinadas personas durante un periodo concreto. Por lo cual, estos datos dan a conocer detalles precisos de la vida privada de las personas cuyos datos se conservan, como por ejemplo los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios, las relaciones sociales y los medios sociales frecuentados.

Las principales consideraciones que expone el Tribunal de Justicia en las sentencias de asuntos acumulados C-293/12 Y C-594/12[63] del 8 de abril de 2014, para declarar inválida la Directiva, se resumen en los siguientes puntos:

1. El Tribunal de Justicia, consideró que la Directiva, al permitir que se conserven determinados datos y que estos sean proporcionados a las autoridades nacionales competentes, configura una intromisión grave en la vida privada de las personas, afectando los derechos fundamentales al respeto a la vida privada y a la protección de los datos de carácter personal dado que la conservación y posterior utilización de los datos se efectuaba sin que el usuario registrado fuera informado de ello, lo que genera en los ciudadanos la sensación de estar bajo constante vigilancia.

2. El Tribunal reconoció que la Directiva no permitía conocer el contenido de las comunicaciones electrónicas y estableció que los proveedores de servicios o de redes deben respetar ciertos principios de protección y de seguridad de los datos. Adicionalmente, destacó el Tribunal, que el fin que se buscaba con la conservación de los datos, es luchar contra el crimen organizado y preservar la seguridad pública. No obstante, el Tribunal estimó que al establecer la retención de datos, el legislador de la UE sobrepasó los límites del principio de proporcionalidad, en la ponderación de los derechos que se encuentran en colisión. En este sentido, la injerencia de la Directiva en los derechos fundamentales al respeto a la vida privada y a la protección de los datos personales, fue desproporcional frente al objetivo que se perseguía de luchar contra la delincuencia y mantener la seguridad ciudadana.

3. Estimó el Tribunal que la Directiva no fijaba ningún criterio objetivo que garantice que las autoridades competentes únicamente tendrán acceso a los datos, y que se utilicen solamente

[63] Disponibles en el Link http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130de9ebfa00a2fbd40fbbb73ef4a1e526835.e34KaxiLc3eQc40LaxqMbN4Ob30Me0?text=&docid=150642&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=437487

con el fin de prevenir, detectar, reprimir, delitos de gran magnitud, que justifiquen la injerencia en los derechos fundamentales de los ciudadanos. Por el contrario, la Directiva solo hacía una remisión a los delitos graves, definidos por cada Estado miembro en su ordenamiento jurídico interno. Adicionalmente, la Directiva no estableció un control previo de una autoridad jurisdiccional o administrativa autónoma, y tampoco define las condiciones procesales y materiales, en las que las autoridades judiciales y las agencias de inteligencia acceden y usan los datos posteriormente.

4. Consideró el Tribunal que no eran adecuados los términos en que se contemplaba el periodo de conservación de datos, puesto que el artículo 6 de la Directiva contemplaba un periodo entre seis meses como mínimo y veinticuatro meses como máximo, sin que se gradúe el tiempo de retención, ni se precisaran criterios objetivos que determinaran un periodo de retención estrictamente necesario, distinguiendo las categorías de datos en función de las personas afectadas o del uso que se dé a los datos de acuerdo al delito que se persigue.

5. Identificó el Tribunal que la Directiva no garantiza una protección eficaz de los datos personales, contra los inminentes riesgos de acceso y uso ilícito de estos, puesto que la Directiva no aseguraba que cuando culminaba el termino de conservación de los datos, estos fueran borrados o destruidos.

6. Finalmente, el Tribunal consideró inadmisible que la Directiva no obligara a los operadores a conservar los datos en el territorio de la UE, lo que evidencia ausencia de mecanismos de protección efectivos por parte de una autoridad independiente, como lo exige la Carta, ya que dicho control debe materializarse de acuerdo con lo que establece el Derecho de la Unión, que es un elemento esencial del respeto a la protección de las personas en relación con el tratamiento de los datos personales.[64]

## 5.2 España

En España el propósito de la Estrategia de Ciberseguridad Nacional , promovida por el Consejo de Seguridad Nacional, es fijar las directrices generales del uso seguro del ciberespacio con la colaboración de todos los agentes involucrados en el proceso, como son las administraciones públicas, la industria y los ciudadanos, dando cumplimiento a la estrategia de Ciberseguridad de la UE.

[64]Puede ser consultada en el link http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054es.pdf

Las principales medidas para alcanzar los objetivos señalados en la Estrategia de Ciberseguridad Nacional, se resumen en la siguiente tabla:

**Tabla No. 4 Líneas de Acción de la Ciberseguridad Nacional en España[65]**

| LÍNEA DE ACCIÓN | | CONTENIDO |
|---|---|---|
| 1 | Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas | Incrementar las capacidades de prevención, defensa, detección, análisis, respuesta, recuperación y coordinación ante las ciberamenazas, haciendo énfasis en las administraciones públicas, las infraestructuras críticas, las capacidades militares y de defensa y otros sistemas de interés nacional. |
| 2 | Seguridad de los sistemas de información y telecomunicaciones que soportan las administraciones públicas | Garantizar la implantación del Esquema Nacional de Seguridad, reforzar las capacidades de detección y mejorar la defensa de los sistemas clasificados. |
| 3 | Seguridad de los sistemas de información y telecomunicaciones que soportan las Infraestructuras Críticas | Impulsar la implantación de la normativa sobre protección de infraestructuras críticas y de las capacidades necesarias para la protección de los servicios esenciales. |
| 4 | Capacidad de persecución del ciberterrorismo y la ciberdelincuencia | Potenciar las capacidades para detectar, investigar y perseguir las actividades terroristas y delictivas en el ciberespacio, sobre la base de un marco jurídico y operativo eficaz. |
| 5 | Seguridad y resiliencia de las TIC del sector privado | Impulsar la seguridad y la resiliencia de las infraestructuras, redes, productos y servicios empleando instrumentos de cooperación público privada. |
| 6 | Conocimientos, Competencias e I+D+i | Promover la capacitación de profesionales, impulsar el desarrollo industrial y reforzar el sistemas I+D+i en materia de ciberseguridad. |

[65] Estrategia de Ciberrseguridad Nacional. Gobierno de España. Presidencia del Gobierno. 2013. Pág. 40. Disponible en https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ES_NCSS.pdf

| | | |
|---|---|---|
| 7 | Cultura de la ciberseguridad | Concientizar a los ciudadanos, profesionales y empresas de la importancia de la ciberseguridad y el uso responsable de las TIC y de los servicios que integran la sociedad de la información. |
| 8 | Compromiso internacional | Promover un ciberespacio internacional seguro y confiable, en apoyo a los intereses nacionales. |

Después de la expedición de la Directiva 2006/24/CE, el gobierno español aprobó la Ley 25 de 2007 *"De conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones",* sin embargo es importante tener en cuenta que con la declaratoria de anulación de la Directiva 2006/24/CE por parte del Tribunal de Justicia de la Unión Europea (TJUE), se afectan las Leyes que los estados miembros hayan adoptado para dar cumplimiento a lo establecido en la Directiva, puesto que es posible que sobrevenga la posible nulidad de la normativa nacional que traspone la norma comunitaria.

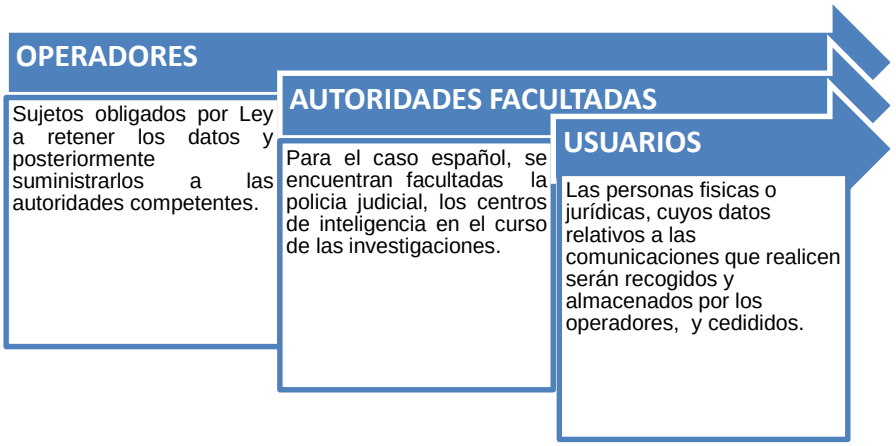
No obstante, se hará referencia a la Ley 25 de 2007, a través de la cual el gobierno español estableció la obligación de los operadores de conservar determinados datos, con el fin de luchar contra el terrorismo, la delincuencia organizada y una serie de delitos, que pueden generarse en el curso de las comunicaciones electrónicas y en el uso de redes públicas[66]. De acuerdo a lo anterior, la Ley 25 de 2007 establece la conservación de datos con un doble objeto:

1. Imponer a los operadores la obligación de conservar los datos de tráfico, localización e identificación de usuarios.
2. Regular los términos de la cesión de los datos a las autoridades policiales al amparo de la correspondiente autorización judicial y para fines de detección, investigación y enjuiciamiento de delitos graves[67].

Las medidas descritas, afectan a los operadores, a los usuarios y a las autoridades policivas o jurisdiccionales que van a usar los datos, de la manera como se describe en el siguiente gráfico.

[66] La principal finalidad en la conservación de estos datos se da cuando las autoridades policiales y judiciales, reclaman tales datos a los operadores y los usan en el curso de una investigación, con el fin de prevenir y perseguir delitos graves.
[67] Se limita el alcance de la cesión de los datos, a la investigación y enjuiciamiento de "delitos graves", de acuerdo a lo que establece el Código Penal. Sin embargo se contempla una excepción a esta regla, puesto que la Ley 27 señala que la obligación de identificación de los usuarios de los servicios de telefonía mediante tarjetas prepago tiene como finalidad "*… la investigación, detección y enjuiciamiento de un delito",* sin que este se califique con la categoría de grave.

**Gráfico 12**. Agentes involucrados en la retención de datos de acuerdo a la Ley 25 de 2007




El artículo 3 de la Ley 25 de 2007, establece que los datos que deben conservarse son los datos de tráfico, localización y otros datos necesarios para identificar al abonado o usuario registrado, pero en ningún caso incluye los datos relativos al contenido de las comunicaciones. La norma española prácticamente transcribe el listado de la Directiva 24/2006/CE[68].

Por otra parte, en la actualidad España realiza un estudio[69] referente a la necesidad de certificación y acreditación en materia de Ciberseguridad, que comprende tres herramientas de estructuración:

1. Certificaciones de seguridad intrínseca a equipos y aplicaciones informáticas: Certificar en principio a equipos como ordenadores, impresoras, routers, firewalls, etc. y aplicaciones informáticas de ofimática, de contabilidad, de control de procesos, páginas web etc. con una etiqueta que indique que es un equipo o aplicación "segura" basada en los denominados Common Criteria.[70]
2. Exigir acreditación de la seguridad de sistemas informáticos en operación: se pretende definir un Sistema de Gestión de la Seguridad de la Información (SGSI), en el cual se definen los

[68] Este listado comprende los datos necesarios para: (i) rastrear e identificar el origen y el destino de la comunicación; (ii) determinar su fecha, hora y duración; (iii) identificar el tipo de comunicación y el equipo de comunicación utilizado; e (iv) identificar la localización en los casos de equipos de comunicación móvil.
[69] ESYS. "Estudio sobre las necesidades de certificación y acreditación en materia de ciberseguridad". Madrid, Noviembre de 2013.Disponible en http://www.fundacionesys.com/files/Estudio%20ESYS_Ciberseguridad.pdf.
[70]Estos criterios son un conjunto de normas redactadas como consenso, por una serie de organismos nacionales de Australia Nueva Zelanda, Canadá, Francia, Alemania, Japón, Holanda, Gran Bretaña, Estados Unidos y España. http://www.commoncriteriaportal.org/cc/

procedimientos a seguir para una buena práctica de gestión, todo ello de acuerdo a la norma ISO 27001.[71]

3. Exigir acreditaciones a los técnicos y directivos que trabajen en Ciberseguridad.

### 5.3 Reino Unido

Después de que el Tribunal de Justicia de la UE (TJUE) el pasado 8 de abril de 2014 declarara invalida la Directiva que establecía las reglas para la conservación de datos en relación con la prestación de servicios de comunicaciones electrónicas (Directiva 2006/24/CE), el gobierno británico anunció el 10 de julio la preparación de una legislación de emergencia para seguir vigilando internet y las llamadas telefónicas, lo que ha alarmado a los defensores de los derechos civiles por considerarlo una amenaza a la privacidad[72].

El Proyecto se presentó al Parlamento para que fuera aprobado lo más pronto posible[73], para que se obligue a los proveedores de servicios de telecomunicaciones, a conservar los datos de los correos y las llamadas de los clientes. Sin embargo, el gobierno aclaró que se restringirá el número de organizaciones que podrán acceder a la información, puesto que está información se usará para mantener la seguridad del País.

La medida de urgencia, se adopta principalmente por el temor a que la información que ya ha sido retenida por los proveedores, sea destruida debido a que el TJUE declarara invalida la Directiva 2006/24/CE, lo que impediría el uso de la información retenida para judicializar criminales y combatir el terrorismo.

Finalmente se aclaró que el proyecto de ley *"Poderes de Investigación y Retención de Datos"*, no permite acceder al contenido de las comunicaciones, sino a los datos sobre la fecha, la hora y el día en que se hicieron las comunicaciones.

---

[71] Es un estándar internacional para la seguridad de la información (*Information technology - Security techniques - Information security management systems - Requirements*), aprobado y públicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.Este estándar especifica los requisitos necesarios para implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI). Disponible en http://www.iso.org/iso/catalogue_detail?csnumber=42103.

[72] Miembros del grupo "Liberty" y del "Open Rights Group", consideran que dicha legislación esta destina a espiar a todos y no solo a los sospechosos de terrorismo, consideran que el gobierno británico encuentra como pretexto una amenaza terrorista, para aprobar una Ley de emergencia que infringe evidentemente el derecho a la privacidad.

[73] Actualmente el Proyecto de Ley debe surtir varios debates, sin embargo, es importante señalar que de ser aprobada la Ley está será efectiva hasta el año 2016. http://noticias.lainformacion.com/politica/ejecutivo-gobierno/londres-presenta-una-ley-para-autorizar-la-retencion-de-datos-de-comunicaciones_KmqhlsleDFJB7ctd3gB4l4/.

Es importante señalar que los principales lineamientos que establece la agenda regulatoria 2015 de OFCOM, en materia de ciberseguridad son:

I. Llevar a cabo acciones, programas y proyectos que permitan implantar sistemas tecnológicos que hagan más resistente la red, promover la seguridad informática y el acceso a los servicios de emergencia.
II. Evaluar el riesgo y determinar la capacidad de recuperación de la red cibernética.

### 5.4 Finlandia

Finlandia inició el año 2015 con la entrada en vigencia de un nuevo Código de la Sociedad de la Información, adoptada mediante la Ley 917 de 2014[74] que actualiza la legislación de las comunicaciones electrónicas del país. La ley tiene cuatro objetivos principales: la simplificación de las normas existentes, mejorar la protección de los consumidores, impulsar la seguridad de la información y crear mercados más equitativos de telecomunicaciones. La norma supone medidas directas para las redes sociales y proveedores de mensajería online, por delante de la gran revisión que prepara la Unión Europea en este año[75].

La nueva ley también regula los contenidos de los llamados operadores Over the Top en lo que se refiere a privacidad y seguridad; las disposiciones se aplicarían a cuestiones tales como intercambio de mensajes confidenciales a través de medios de comunicación social. Este es un pequeño paso hacia la igualdad de condiciones entre los operadores de telecomunicaciones tradicionales y los nuevos actores de Internet.

Esta norma ha llamado la atención mundial debido a que la disposición implica que empresas como Apple, Facebook o Twitter deberán asegurarse que los usuarios de sus servicios de mensajería obtengan los mismos estándares de privacidad y seguridad que compañías ya reguladas como las empresas de telecomunicaciones y los proveedores de servicios de valor agregado. Otro aspecto novedoso, es que dicha normativa refuerza la protección del consumidor, por ejemplo, cuando un consumidor compra un producto o servicio con su teléfono móvil y el pago se realiza a través del operador de telecomunicaciones, este proveedor compartirá la responsabilidad con la empresa que vende el producto o servicio, si surgen problemas con la compra, el consumidor puede recurrir a cualquiera de las empresas en busca de ayuda."[76]

---

[74] https://www.finlex.fi/sv/laki/ajantasa/2014/20140917
[75] http://www.siliconnews.es/2015/01/05/finlandia-introduce-nueva-ley-para-la-privacidad-en-las-comunicaciones-electronicas/
[76] Código de la Sociedad de la Información de Finlandia protege privacidad. Media Telecom.http://goo.gl/xrJr7d

## 5.5 Estados Unidos

Para Estados Unidos la seguridad nacional y económica del país depende en gran medida del funcionamiento fiable de su infraestructura crítica, por tal razón, durante los últimos años se han adelantado diferentes medidas asociadas a implementar una estrategia que permita la defensa de la infraestructura crítica del país contra ataques cibernéticos.

En el año 2008 fue lanzada la Iniciativa Integral Nacional de Ciberseguridad (CNCI)[77] por sus siglas en inglés) en la que posteriormente se adelantó en 2011 una revisión general que determinó que el CNCI y sus actividades conexas debería evolucionar para convertirse en elementos clave de una estrategia más amplia de seguridad cibernética nacional de Estados Unidos, así:

- Establecer una línea de defensa contra las amenazas inmediatas, mediante la creación o mejora de la conciencia compartida de vulnerabilidades de la red, las amenazas y eventos dentro del Gobierno Federal, y en última instancia con sectores estatales, locales y tribales y los socios del sector privado, y la posibilidad de actuar con rapidez para reducir vulnerabilidades actuales y prevenir intrusiones.
- Defenderse de todo el espectro de amenazas mediante la mejora de las capacidades de contrainteligencia de Estados Unidos y el aumento de la seguridad de la cadena de suministro de las tecnologías de información clave.
- Fortalecer el futuro entorno de la ciberseguridad al expandir la educación cibernética; la coordinación y la reorientación de los esfuerzos de investigación y desarrollo en todo el Gobierno Federal; y trabajando para definir y desarrollar estrategias para disuadir la actividad hostil o maliciosa en el ciberespacio.

Es así como en el año 2013 se emitió la Orden presidencial[78] que presenta lineamientos para prevenir y disipar los ciberataques y perturbaciones en las redes que soportan las funciones consideradas críticas e incluye estrategias el mejoramiento en la prevención, detección y respuesta a los incidentes cibernéticos de tal forma que la información sobre los ataques pueda aprovecharse para la defensa.

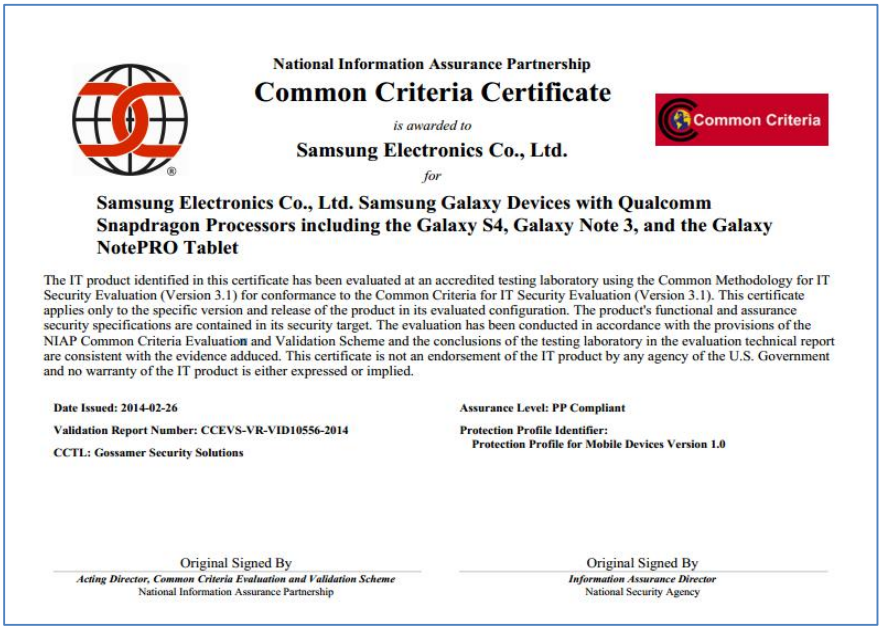
Según las cifras de la Agencia Nacional de Seguridad (National Security Agency -NSA) de 2013 la cantidad de datos que circulan al día por internet son de 1,828 Petabytes. De los cuales la NSA solo puede captar 1,2 % y de ellos solo una fracción se da a conocer, esto sería solo el 0,0004 % del total

[77] Directiva Nacional de Seguridad Presidencial 54 / Homeland Security Presidential Directive 23 (NSPD-54 / HSPD-23)
[78] Executive Order -- Improving Critical Infrastructure Cybersecurity https://m.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

de la circulación de datos, y solo en ellos se coloca el filtro de búsqueda de las autoridades. No obstante las preocupaciones a nivel nacional e internacional, respecto al papel de la NSA en el seguimiento de información personal y corporativa, llevaron a una gran preocupación sobre el alcance de acción de dicha entidad. Es así como en enero de 2014 el Presidente Obama anunció unas medidas de reducción de daños[79] al establecer que la recolección de datos solo para fines de política de seguridad, los datos de telecomunicación de los americanos deberán ser grabados en el futuro solo por el proveedor, y el acceso para la NSA solo se puede dar por orden judicial.

De otra parte, en cuanto a temas particulares para la industria TI y los equipos terminales, respecto a seguridad, se han adoptado certificaciones expedidas por instancias como la NIAP (National Information Assurance Partnership), la cual es una iniciativa del gobierno de Estados Unidos para identificar las necesidades de pruebas de seguridad tanto de consumidores como de productores de tecnologías de la información, la cual es operada por la NSA y fue el resultado de un esfuerzo conjunto entre la NSA y el NIST (National Institute of Standards and Technology) de Estados Unidos.

**Gráfico. No. 13** Certificado de cumplimiento de Criterios Comunes expedido por NIAP



National Information Assurance Partnership

**Common Criteria Certificate**

*is awarded to*

**Samsung Electronics Co., Ltd.**

*for*

**Samsung Electronics Co., Ltd. Samsung Galaxy Devices with Qualcomm Snapdragon Processors including the Galaxy S4, Galaxy Note 3, and the Galaxy NotePRO Tablet**

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 3.1) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

**Date Issued: 2014-02-26**

**Validation Report Number: CCEVS-VR-VID10556-2014**

**CCTL: Gossamer Security Solutions**

**Assurance Level: PP Compliant**

**Protection Profile Identifier:**
**Protection Profile for Mobile Devices Version 1.0**

Original Signed By
*Acting Director, Common Criteria Evaluation and Validation Scheme*
National Information Assurance Partnership

Original Signed By
*Information Assurance Director*
National Security Agency

Fuente: NIAP

[79] https://www.whitehouse.gov/sites/default/files/docs/2014sigint_mem_ppd_rel.pdf

Los Criterios Comunes (CC) proporcionan un conjunto común de requisitos funcionales para los productos de TI (Tecnologías de la Información) que surgieron como resultado de la armonización de los criterios sobre seguridad de productos software utilizados por diferentes países con el fin de que el resultado del proceso de evaluación pudiese ser aceptado en múltiples países. Los CC combinan criterios de los sistemas de evaluación de seguridad de Estados Unidos, Canadá y Europa, y fueron adoptados por la International Organization for Standardization (ISO) bajo la serie de normas ISO/IEC 15408.

El proceso de evaluación establece un nivel de confianza en el grado en el que el producto TI satisface la funcionalidad de seguridad de estos productos y ha superado las medidas de evaluación aplicadas.

### 5.6 Australia

En noviembre de 2009 en Australia se creó la Estrategia de Ciberseguridad (CSS, por sus siglas en inglés). La CSS estableció las prioridades estratégicas del gobierno para asegurar la Infraestructura de Información Nacional (NII, por sus siglas en inglés) y reunió dos iniciativas: el CERT (Computer Emergency Response Team) Australia y el CSOC (Cyber Security Operations Centre) que iniciaron operaciones en 2010.

La red de cooperación de información confiable (TSIN – Trusted Information Sharing Network) representa los mayores grupos del sector que han sido identificados como infraestructura crítica para los intereses de seguridad nacional. Estos incluyen: banca y financiero, comunicaciones, energía, cadena de alimentos, salud, transporte y agua. El CERT Australia trabaja muy de cerca con el TISN para asesorar y asistir a los miembros del grupo en estrategias para la protección contra ciber ataques.

Por otra parte, el ente regulador ACMA (Australian Communications and Media Authority) desarrolló la iniciativa de seguridad en Internet australiana (AISI) para ayudar a controlar el problema de los computadores infectados por algún tipo de malware (los cuales son conocidos como zombies, bots o drones). Los equipos pueden ser infectados a través de la instalación oculta de software malicioso que permiten a los computadores ser controlados remotamente para realizar actividades peligrosas e ilegales sin el conocimiento del dueño del computador.

Los equipos comprometidos (infectados) comúnmente son agregados en grandes grupos de "botnets". Entre otras cosas, los botnets son utilizados para colaborar en la distribución masiva de spam y malware, el alojamiento de sitios de phishing y ataques de DDoS (Denegación de Servicio distribuida).

El AISI reúne datos de varias fuentes en computadores que presentan un comportamiento de "bot" dentro de las redes de Internet australianas. A partir de estos datos, el ACMA provee reportes diarios para los ISP identificando las direcciones IP en sus redes que, a su vez, han sido reportadas al ACMA en las 24 horas anteriores. Los ISP pueden así informar a sus usuarios asociados a dichas IP que sus computadores parecen estar comprometidos y dan sugerencias sobre la forma de solucionarlo.

Actualmente participan 139 miembros, incluyendo 18 universidades, con los cuales se estima está cubierto el 90% de los usuarios residenciales de Internet. El ACMA busca aumentar progresivamente la participación de los ISP en el AISI, para ello deben suministrar las direcciones IP y los números de Sistemas Autónomos.

En Australia es ilegal que cualquier persona u organización utilice y controle remotamente el computador de otra persona sin su consentimiento. Bajo el Código Criminal 1995 las penas aplican en las siguientes circunstancias:

1. Acceso no autorizado y modificación de los datos a través de algún servicio de comunicación: Por ejemplo, acceder al computador de otra persona para instalar un bot. Pena máxima de dos años de prisión.
2. Modificación no autorizada de datos a través de algún servicio de comunicación. Por ejemplo, instalar un bot en el computador de otra persona. Pena máxima de 10 años de prisión.
3. Posesión de datos con el propósito de cometer un delito informático. Por ejemplo, posesión de códigos de bot, herramientas de exploit[80] o instaladores. Pena máxima de 3 años de prisión.
4. Producción, distribución u obtención de datos con el fin de cometer delitos informáticos. Por ejemplo, desarrollar o vender código de bot. Pena máxima de 3 años de prisión.

El ACMA reporta la información de tales actividades criminales al Centro Australiano para Crímenes de Alta Tecnología o la fuerza de policía del estado o territorio[81].

### 5.7 Chile

Dentro de la Agenda Digital Imagina Chile, la cual es la estrategia de desarrollo digital de Chile para el periodo 2013-2020, se han planteado iniciativas para fomentar el uso de las Tecnologías de la

[80] Exploit (del inglés to exploit, 'explotar' o 'aprovechar') es un fragmento de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo. Los exploits pueden tomar forma en distintos tipos de software como por ejemplo scripts, virus o gusanos informáticos.

[81] http://www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/australian-internet-security-initiative

Información y las Comunicaciones (TIC), mejorar la competitividad de los países y la calidad de vida de sus ciudadanos.

Una de las iniciativas es la de ofrecer seguridad para el ciudadano en el mundo digital, cuyo objetivo es promover un marco de confianza que favorezca el desarrollo de los servicios digitales. Para ello se procurará la protección adecuada del usuario en las operaciones y transacciones que realiza en la red; los derechos del consumidor en la red se abordarán con una visión integral y sistémica, lo que implicará una evolución del marco normativo que tiene como base la Ley de Protección al Consumidor (Ley 19.496 del 1997 que establece las normas sobre la protección de los derechos de los consumidores).

Otro objetivo es el tratamiento de la privacidad y manejo de datos personales, con el fin de alcanzar un balance entre la protección de estos derechos y el aseguramiento del acceso a la información. Para ello se está adelantando actualmente un proyecto de ley en el Congreso: *"Protección de datos personales Boletín No. 8143-03, que introduce modificaciones a la Ley No. 19.628 Sobre protección de la vida privada"* con el objeto de adecuar la normativa a estándares internacionales sobre privacidad y flujos transfronterizos de datos personales, teniendo presente el gran desafío global que representa la protección de la privacidad en internet.

Por otro lado, en un contexto en el que los delitos informáticos son generados desde cualquier país del mundo y son muy difíciles de rastrear, el rol regulador y fiscalizador del Estado cobra una mayor importancia en materia de Ciberseguridad y delitos informáticos.

Lo anterior se traducirá en una acción proactiva en la identificación y eliminación de amenazas y fraudes potenciales en materia digital. Este rol del Estado es crítico en materia de protección infantil, para lo que, además de regular, se promoverá una cultura de respeto mutuo a través del involucramiento familiar en el proceso de aprendizaje digital.[82]

Actualmente se planea un Centro Nacional de Mando para el manejo de situaciones de crisis, emergencias y amenazas, que estará adscrito al Ministerio del Interior y Seguridad Pública, y adicionalmente estará directamente subordinado a la Presidencia de la República.

El nuevo Centro Nacional de Mando, asumirá tareas de inteligencia hasta ahora asignadas por Ley a la Agencia Nacional de Inteligencia (ANI), y en esta medida creara un Centro de Ciberseguridad, que estará bajo una directa dependencia de la jefatura del Ministerio del Interior y Seguridad Pública. El

[82] Consultado en el link: http://www.desarrollodigital.gob.cl/AgendaDigitalImaginaChile.pdf

centro de ciberseguridad tendrá a su cargo, las investigaciones relacionadas con el uso del ciberespacio como medio de comunicación, atender los ataques a la infraestructura digital del Estado, atender las solicitudes de emergencia de incidentes informáticos de las entidades del Estado, realizar las investigaciones y judicializar los crímenes contra la infraestructura critica del Estado[83].

En el terreno de la seguridad y la protección, Chile ha iniciado un proceso tras ser invitado a ser parte de la Convención de Budapest, con el ánimo de adherir al esfuerzo de los estados miembros del Consejo de Europa y otros estados firmantes, para homologar la legislación en materia de cibercrimen y facilitar su persecución, sobre todo atendiendo la transnacionalidad de estos delitos.

### 5.8 México

En julio de 2014 se promulgaron las leyes secundarias de la reforma de telecomunicaciones, y se impuso a los concesionarios de telecomunicaciones la obligación de proporcionar la localización geográfica en tiempo real de cualquier tipo de dispositivo de comunicación involucrado en las investigaciones que cursen para combatir delitos como el secuestro, extorsión, terrorismo, etc.

Por otra parte, se estableció a los operadores la obligación de conservar por 24 meses un registro y control de comunicaciones que se realicen desde cualquier dispositivo y modalidad, que incluya la información del suscriptor, así como el origen, el destino, la fecha y la hora de la comunicación.[84]

Adicionalmente, en junio de 2014 México firmó en España el **Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia[85],** que fortalece los instrumentos de cooperación internacional y contribuye a la modernización de legislaciones penales en la materia. Se pretende combatir delitos como el acceso no autorizado a un sistema informático y el robo de información; fabricar y vender dispositivos falsificados con códigos de acceso; producción de pornografía infantil; plagio de obras literarias, artísticas o científicas, y suplantar la identidad, entre otras.

---

[83] Consultado en el Link: http://www.infodefensa.com/latam/2014/02/26/noticia-chile-creara-centro-nacional-mando-ciberseguridad.html

[84] El Proyecto de Ley aprobado puede consultarse en el siguiente Link http://www.presidencia.gob.mx/wp-content/uploads/2014/03/INICIATIVA-LEY-CONVERGENTE.pdf. El artículo 196 y siguientes contemplan las obligaciones descritas.

## 5.9 Israel

Israel ha sido catalogado como una potencia mundial e innovadora (Innovation Nation) por la UIT-T, y ha implementado una gran estrategia nacional de Ciberseguridad. De la estrategia se pueden identificar cinco pilares fundamentales en los cuales basa el éxito de la concentración de talento en la industria de la Ciberseguridad[86]:

(i) el fortalecimiento de las fuerzas armadas y las de seguridad aseguran una masa crítica de mercado para los desarrolladores de esta materia,
(ii) Universidades e Institutos de primer nivel que garantizan el mejor nivel de aprendizaje en la materia,
(iii) facilitación del flujo de información y el desarrollo de nuevas ideas y aplicaciones en la materia,
(iv) alfabetización y promoción del conocimiento científico,
(v) alerta constante ante la delicada situación geopolítica del Estado de Israel

Como se muestra y comentan en muchos espacios *"El ejemplo de Israel muestra que cuando los gobiernos actúan con prioridades a largo plazo planificando la estrategia de desarrollo del país en base a sus fortalezas, todas las partes se ven beneficiadas, el propio gobierno, los institutos de enseñanza, las empresas privadas, los individuos y finalmente la sociedad toda que recibe los beneficios de la interacción de todos estos actores*". [87].

En Colombia en la actualidad se llevan a cabo acercamientos con los representantes en temas de Cbierseguridad y Ciberdelito de Israel con el fin de recibir apoyo y recomendaciones sobre el desarrollo de la formulación de la nueva estrategia de Ciberseguridad y Ciberdefensa para el país, de ahí se debe identificar que para un planteamiento adecuado se debe tener en cuenta las buenas prácticas de Israel como el fortalecimiento de la defensa y la construcción de la fuerza nacional en el ámbito cibernético, la creación de liderazgo en el campo cibernético y avanzar en los procesos que soportan las dos primeras tareas como lo hace el The National Cyber Bureu de Israel[88]

[86] http://e-volucion.elnortedecastilla.es/actualidad-digital/israel-un-viaje-la-ciber-nacion-12032014.html
[87] Parafraseando a Simon Peres, Premio Nobel de La Paz, dos veces Primer Ministro y actual Presidente de Israel, Consultado en: http://e-volucion.elnortedecastilla.es/actualidad-digital/israel-un-viaje-la-ciber-nacion-12032014.html
[88] The National Cyber Bureu de Israel, Consultado en : http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/default.aspx

En la reciente participación de Israel en el congreso CiberColombia 2015 "Concepto y Tecnología de Ciberdefensa y Ciberinteligencia para las fuerzas militares e Infraestructura Nacional" se expuso[89] como la estrategia nacional de Israel continúa enfocando esfuerzos en el aumento de las capacidades tecnológicas y una infraestructura científica en el país. Para lograr esto, se lleva a cabo un trabajo en conjunto con la industria, el estado y la academia con el fin de lograr la preparación necesaria y capacitación para lograr contrarrestar los múltiples ataques y múltiples métodos utilizados.

### 5.10 Consideraciones

De la situación internacional expuesta se puede observar que los temas de mayor relevancia y atención en cuanto a Ciberseguridad y Ciberdefensa son:

- Adecuación del marco normativo (protección de datos, protección a usuarios, interceptación de comunicaciones, retención de datos etc.) en materia de ciberseguridad y ciberdefensa, que atienda las necesidades actuales y que busque la protección adecuada del usuario en las operaciones y transacciones que realiza en la red.
- Formulación de medidas y herramientas efectivas que fortalezcan la capacidad de prevención, respuesta y recuperación ante ciberamenazas y ciberataques.
- Identificación de infraestructuras críticas, así como el establecimiento de medidas más efectivas para prevenir ciberataques y/o mitigar sus efectos sobre estas, con el fin de asegurar la continuidad en la prestación de los servicios esenciales.
- Adopción de medidas efectivas que fortalezcan la seguridad y la resiliencia de las infraestructuras, las redes, los productos y servicios, empleando instrumentos de cooperación público-privados.
- Promover la cooperación internacional para la protección del ciberespacio.

## 6. PROPUESTA DE ACCIONES A TENER EN CUENTA EN LA FORMULACIÓN DE LA NUEVA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD Y CIBERDEFENSA

A partir de lo expuesto en las secciones anteriores, se identifica la concordancia existente a nivel internacional en las áreas que se consideran relevantes para tener en cuenta en el trabajo que se adelante para la estructuración de una nueva estrategia nacional de Ciberseguridad y Ciberdefensa. Es así como se plantean cinco líneas de acción que deberían contemplarse en la estrategia antes

[89] Exposición de Michael Levinrad, representante de la Autoridad Nacional de Cibernetica del despacho del primer ministro del estado de Israel. Bogotá, mayo 19 de 2015.

indicada, las cuales corresponden a: i) Aspectos normativos, ii) Aspectos técnicos, iii) Procedimientos, iv) Capacitación e información, y v) Cooperación internacional.

De las diferentes temáticas expuestas a lo largo del documento se plantea una propuesta de aspectos a desarrollar que pueden contribuir al fortalecimiento de la nueva estrategia nacional de Ciberseguridad y Ciberdefensa, los cuales pueden ser adelantados por diferentes Entidades según el ámbito de sus competencias. En este caso, para las cinco áreas de trabajo, la CRC identificó y planteó tres (3) temas a tratar, teniendo en cuenta el estudio adelantado y el análisis de la información recopilada sobre recomendaciones planteadas por los diferentes organismos y el impacto que genera en los usuarios TIC:

1. Seguridad de Redes
2. Protección de Datos del Usuario
3. Procedimientos para la investigación de delitos informáticos/ Preservación de evidencia digital

Dentro de cada área existen diferentes temáticas que pueden ser atendidas por una o varias Entidades de gobierno, y a su vez es importante recalcar que para lograr sinergia y la definición de actividades y lineamientos con un mayor alcance, se requerirá del trabajo y acompañamiento de las empresas prestadoras del servicios de telecomunicaciones, del sector privado y de la academia. En el Gráfico no. 14 se indican las líneas de acción y los actores de gobierno que participan en la formulación de la estrategia en cuestión.

**Gráfico. No. 14 Mapa de actores – propuesta áreas a tratar en nueva Estrategia Nacional de Ciberseguridad**


Fuente: Elaboración CRC

Con base en el análisis adelantado por la CRC, en la siguiente tabla se consolidan recomendaciones para los tres temas relevantes en relación con cada una de las cinco líneas de acción, descritas, principalmente, desde el punto de vista de la labor de la CRC. Es de indicar que esta es una aproximación realizada por la CRC, sujeta a revisión y validación de cada entidad, por lo cual sólo constituye una propuesta para análisis interinstitucional.

**Tabla No. 5 –Posibles temáticas a ser abordadas para fortalecer la estrategia nacional de ciberseguridad y ciberdefensa**

| | | **Seguridad de Redes** | **Protección de Datos del Usuario** | **Procedimientos para la investigación de delitos informáticos/ Preservación de evidencia digital** |
|---|---|---|---|---|
| **Frente de Acción** | **Normativo** | Fortalecer medidas, y fomentar la adopción de estándares con referentes internacionales para garantizar redes de telecomunicaciones más seguras, incluyendo prestadores de servicios y sector privado. | Formular una reglamentación clara aplicable a los PRST en temas relacionados a retención y protección de datos de los usuarios de los servicios de Telecomunicaciones.<br><br>Identificar medidas de seguridad adicionales que debieran ser adoptadas por los proveedores de servicios encaminadas a garantizar claramente los derechos fundamentales de habeas data y de intimidad. | Reglamentar de una manera amplia y clara los procedimientos de cesión de datos a las autoridades de inteligencia y contrainteligencia y garantizar los derechos fundamentales de habeas data y de intimidad.<br><br>Efectuar la definición de la cadena de custodia de la información almacenada por mandato legal. |
| | **Procedimientos** | Establecer puntos púnicos de contacto en los PRST para dar respuesta oportuna a requerimientos dentro de investigaciones.<br><br>Coordinar con el sector privado, la identificación de las mejores prácticas de seguridad aplicadas y posibles mejoras a implementar.<br><br>Evaluar el cumplimiento por parte de los PRST respecto a las obligaciones de cadena de custodia de la información y datos retenidos al interior de los PRST | Desarrollar medidas que garanticen la confidencialidad de la información almacenada en redes de los PRST, y procedimientos de auditoría de procesos aplicable.<br><br>Definir y clasificar los límites que encuentran los usuarios en el ejercicio para hacer valer sus derechos, relativos al acceso y cancelación de los datos que cursan en las comunicaciones | Definir un procedimiento de preservación de evidencia digital, incluyendo aspectos de destrucción de datos retenidos, una vez se extinga el término de retención. |

| | | | | |
|---|---|---|---|---|
| | **Aspectos Técnicos** | Determinar las medidas técnicas que se deben adoptar para garantizar la protección y confiabilidad de los datos de usuarios, en los diferentes sectores.<br><br>Evaluar las recomendaciones y estándares técnicos sobre seguridad informática (UIT, IEEE, ETSI, ISO) y presentar recomendaciones. | Mediante la elaboración de un documento de estudio definir cuáles serán los estándares y mejores prácticas a usar por parte de los PRST y los Fabricantes de tecnología para garantizar la seguridad en dispositivos de comunicaciones.<br><br>Evaluar la posibilidad de modificar los procesos de homologación de equipos de comunicaciones y la inclusión de nuevos tipos de equipos a homologar. | Definir los tipos de comunicaciones y datos asociados que se conservarán a efectos de seguimientos de inteligencia y contrainteligencia. |
| | **Capacitación e Información** | Desarrollar procesos de formación Especializada a personal técnico de empresas y gobierno. | Campañas dirigidas a usuarios sobre su responsabilidad en el manejo seguro de información en redes. | Desarrollar procesos de formación especializada a personal judicial |
| | **Cooperación nacional e internacional** | Fomentar espacios de trabajo intersectoriales articulados, con participación del sector privado y la academia.<br>Analizar la oportunidad de adelantar convenios internacionales de cooperación adicionales a los que se tienen, que fortalezcan la capacidad de análisis y respuesta de los organismos colombianos.<br>Coordinar con Entidades del Estado la atención a aspectos relacionados con los Proveedores de Redes y Servicios de Telecomunicaciones.<br>Entidades participes de temas de Ciberseguridad tales como Mindefensa, Minjusticia, DNP, MinTIC, Policía Nacional, CRC y otras que puedan ser consideradas para prestar el apoyo en la definición de la estrategia. | | |

Fuente: Elaboración CRC

## 7. EL PAPEL DE LA CRC DENTRO DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD Y CIBERDEFENSA

Como se ha evidenciado a lo largo del presente documento, y en general, en la literatura desarrollada respecto a la Ciberseguridad y la Ciberdefensa, son temas cuyo campo de aplicación es bastante extenso, ya que abarca elementos que van desde el diseño, uso e implementación de infraestructuras, hasta las redes, aplicaciones y la información en sí misma; así como los aspectos que se relacionan con la seguridad nacional, como la protección del ciberespacio nacional y la posible definición como escenario de confrontación. Es así como, al realizar un análisis completo de la situación, tanto en Colombia como a nivel internacional en materia de Ciberseguridad, es necesario dividir los múltiples frentes de acción para abarcar las posibles medidas que puedan adoptarse en este sentido.

Por lo anterior, en la matriz de la Tabla No.6 se indican las áreas que pueden tener participación de la CRC desde el ámbito de sus competencias, según las temáticas planteadas en la Tabla no. 5, sin dejar de lado el planteamiento de desarrollos de manera conjunta con otras Entidades de acuerdo a las

facultades legales que cumplen para apoyar la estructuración de la nueva Estrategia Nacional de Ciberseguridad y Ciberdefensa.

**Tabla No. 6 –Áreas temáticas donde la CRC puede contribuir en la estrategia nacional de ciberseguridad y ciberdefensa**

| | | Seguridad de Redes | Protección de Datos del Usuario | Procedimientos investigación de delitos informáticos/ Preservación evidencia digital |
|---|---|---|---|---|
| Frente de Acción | Normativo | CRC | CRC | |
| | Procedimientos | CRC | CRC | |
| | Aspectos Técnicos | CRC | CRC | CRC |
| | Capacitación e Información | CRC | CRC | |
| | Cooperación nacional e internacional | CRC | | |

Fuente: Elaboración CRC

A partir de estas temáticas que la CRC identifica como susceptibles para desarrollar actividades, se plantean a continuación tareas específicas que serán atendidas por la CRC en los próximos años al interior de su agenda regulatoria y de proyectos.

## 7.1 PROTECCIÓN DE DATOS DEL USUARIO

La Ley 1341 de 2009 dispone en el artículo 4 que es función del Estado intervenir en el sector de las TIC, para promover condiciones de seguridad del servicio al usuario final, promoviendo políticas de prevención de fraudes en la red así como la seguridad informática y de redes para el desarrollo del sector. La intervención del Estado en el sector TIC busca proteger los derechos de los usuarios, velando por la calidad, eficiencia y adecuada provisión de servicios.

En el artículo 53 de la Ley 1341 de 2009 se consagra el derecho de los usuarios a recibir protección en cuanto a su información personal, garantizando la inviolabilidad y el secreto de las comunicaciones, y la protección contra la publicidad indebida de acuerdo a lo dispuesto en la Ley.

Adicionalmente, el artículo 22 de la citada Ley 1341 establece que la CRC es la entidad competente para expedir regulación en materia de protección de los derechos de los usuarios de servicios de telecomunicaciones, además de expedir la regulación de redes y de servicios de telecomunicaciones, contemplando entre sus fines el de garantizar la seguridad y la integridad de las mismas.

Ahora bien, la CRC en virtud de las competencias que le han sido asignadas por la Ley, en especial la maximización del bienestar del usuario, ha orientado su labor en reconocer y entender sus principales necesidades y problemáticas frente a la prestación de los servicios de comunicaciones por parte de los proveedores de redes y servicios de telecomunicaciones. Es así como en los últimos años se han fomentado medidas de transparencia que permitan al usuario conocer las distintas condiciones de prestación que ofrecen los operadores, fortaleciendo así la competitividad de estos mercados y el mejoramiento continuo de la calidad de los servicios. Asimismo a partir de la regulación se ha promovido el incremento del uso de las TIC en la relación operador – usuario, y actualmente se trabaja en el establecimiento de un Régimen de Protección de los Derechos de los Usuarios de los Servicios de Comunicaciones que atienda a criterios de simplicidad y claridad, de tal forma que el usuario pueda tener un mayor entendimiento de los derechos y deberes que le asisten.

De igual manera, la CRC en cuanto a temas relacionados a Seguridad de la información, lo cual afecta también la protección de los derechos de los usuarios de telecomunicaciones, deberá tener en cuenta que los PRST son los principales agentes que procesan, transmiten datos e información, en la cadena de valor de la prestación de servicios de comunicaciones. Como se indicó al inicio del documento, el

artículo 44 de la Ley 1621 de 2013, establece que los PRST deben suministrar a los organismos de inteligencia y contrainteligencia, en el desarrollo de una operación autorizada, la siguiente información:

- El historial de comunicaciones de los abonados telefónicos vinculados a una investigación,
- Los datos técnicos de identificación de los suscriptores sobre los que recae la operación, y
- La localización de las celdas en que se encuentran las terminales y cualquier otra información que contribuya a su localización.

Adicionalmente, se establece que los organismos de inteligencia y contrainteligencia garantizaran la seguridad de la información suministrada, por lo cual en la solicitud que se formule a los PRST, se limitará la información requerida a un periodo que no exceda de cinco (5) años. Adicionalmente es importante tener en cuenta que el Decreto 857 de 2014 reglamentario de la Ley 1621 de 2013, no se pronuncia respecto a la obligación contenida en el artículo 44. Sin embargo, se considera que esta disposición legal representa para los PRST una obligación de retención de datos, dado que el PRST debe garantizar que dicha información está disponible cuando así sea requerida por la autoridad competente. Es necesario garantizar que estos datos sean utilizados únicamente con los fines específicos para los cuales han sido almacenados y evitar que se produzcan fugas de información.

Ahora bien, es necesario señalar que en cuanto al tema de interceptación de comunicaciones el Decreto 1704 de 2012 expedido por el Ministerio de TIC, establece las condiciones en virtud de las cuales se pueden interceptar legalmente las comunicaciones, y determina que los PRST deben adoptar tecnología que le permita a los organismos que tienen funciones permanentes de Policía Judicial, previa autorización del Fiscal General de la Nación o su delegado, las labores de interceptación de comunicaciones. Sin embargo, el Decreto también determina que los PRST deben suministrar a la Fiscalía, de forma inmediata, los datos del suscriptor, tales como: la identidad, la dirección de facturación y el tipo de conexión.

De esta manera, para la CRC resulta necesaria la coordinaciónde trabajo entre el Ministerio de TIC y el Ministerio de Defensa, con el fin de determinar los lineamientos y acciones que se deben incluir en el fortalecimiento de la Estrategia de Ciberseguridad nacional. Así mismo, es necesario evaluar cómo están cumpliendo actualmente los PRST con las obligaciones consagradas en el artículo 4 del Decreto 1704 y en el artículo 44 de la Ley 1621 de 2013.

Teniendo en cuenta lo anterior, la CRC considera oportuno adelantar actividades concretas concernientes a los siguientes temas y que deberán ser tenidos en cuenta en la definición de estudios o proyectos regulatorios de la agenda regulatoria del 2016 y posteriores, o actividades continuas enmarcadas dentro de las competencias de la Comisión de Regulación de Comunicaciones:

1. Analizar e incluir dentro del estudio del Régimen de Protección de los Derechos de los Usuarios de la Resolución CRC 3066 de 2011 toda vez que sea necesario, los deberes de información que debe cumplir el PRST en el momento de la contratación y durante su ejecución en relación a los siguientes temas:
    a. Respecto a la información que debe suministrar el PRST[90]. El usuario deberá conocer cuáles son los recursos tecnológicos (aplicaciones, software, etc.) que actualmente implementa el PRST para garantizar la seguridad de la información en las comunicaciones en su red, los riesgos relativos a la seguridad de la red y del servicio contratado, adicionalmente la manera de divulgación de información sobre aplicaciones que puedan ser utilizadas por los usuarios para aumentar los controles a ataques en los dispositivos móviles.
    b. Sobre la autorización que concede el usuario, para el tratamiento, uso, conservación y destino de sus datos personales, debe contemplar la posibilidad de ser entregada a entidades competentes en medio de procesos de investigación.

2. Adelantar un estudio y evidenciar la posibilidad de establecer normativa asociada a:
    a. Definir y especificar los datos que serán objeto de conservación por parte de los PRST y diferenciarlos según categorías y tipos de comunicaciones
    b. Determinar las medidas técnicas que debe adoptar el PRST para garantizar la protección y confiabilidad de los datos retenidos.
    c. Apoyar a la Entidad competente en la definición de los procedimientos y medidas técnicas a tener en cuenta por parte de los PRST para destrucción de los datos retenidos, una vez se extinga el término de retención.

3. Coordinar espacios de trabajo conjunto con los proveedores de redes y servicios de telecomunicaciones que permitan establecer mecanismos para contrarrestar el delito informático.
    a. Desarrollar iniciativas estratégicas transversales a todos los proveedores para contrarrestar ataques a usuarios TIC, tomando referentes internacionales en la materia, tales como las medidas de auto regulación adoptadas por Australia[91]
    b. Determinar cómo el PRST informará las medidas adoptadas para garantizar que los datos solicitados y conservados, estarán seguros y protegidos.

[90] Actualmente el artículo 11.3 de la Resolución CRC 3066 de 2011, establece que el PRST deberá explicarle al usuario lo siguiente: "Señor usuario, usted debe tener en cuenta que existen riesgos sobre la seguridad de la red y el(los) servicio(s) contratado(s), los cuales son (…)".
[91] Buenas prácticas de Australia, referenciadas en el presente documento.

## 7.2 SEGURIDAD DE REDES

La CRC expidió la Resolución CRC 3067 de 2011, en la cual se determina que los PRST deben utilizar los recursos técnicos y logísticos tendientes a garantizar la **seguridad en la red y la integridad del servicio**, por lo cual debe informar en su página web las acciones adoptadas en relación con el servicio prestado al usuario final, tales como el uso de firewalls, filtros antivirus y la prevención del spam, phishing, malware entre otros, y adicionalmente los PRST que ofrezcan acceso a internet deben implementar modelos de seguridad, de acuerdo con los marcos definidos por la UIT.

Teniendo en cuenta lo anterior la CRC se propone adelantar actividades con respecto a:

1. Realizar un diagnóstico en las redes de los PRST para evaluar el alcance técnico del cumplimiento de las medidas establecidas en la Resolución CRC 3067 de 2011 tendientes a garantizar la seguridad en la red, con el fin de determinar y concluir qué tan seguras son las redes en la actualidad, en línea con las recomendaciones internacionales y adopción de un sistema de gestión de riesgos cibernéticos adecuado a los actuales ataques.

2. En complemento al diagnóstico propuesto, identificar la adopción de medidas técnicas actuales, tales como el RFC2827 para evitar ataques de Denegación de Servicio (DoS), y Denegación de Servicio Distribuido (DDoS), así como avances en nuevas medidas de protección frente a las crecientes amenazas.

### 7.2.1 Homologación: Estándares de seguridad de equipos

El capítulo II de la Resolución CRC 3067 de 2011 establece obligaciones de calidad para el servicio de acceso a Internet por parte de los proveedores de redes y servicios de telecomunicaciones; particularmente el artículo 2.3 establece la obligación de utilizar recursos técnicos y logísticos tendientes a garantizar la seguridad en la red y la integridad del servicio para evitar interceptación, interrupción e interferencia del mismo, exceptuando la responsabilidad respecto a los equipos que utilice el cliente, debido a que los mismos no son controlados por los proveedores, sino por los usuarios del servicio.

Es importante tener en cuenta que actualmente los usuarios acceden a internet con más frecuencia desde dispositivos portátiles y móviles, razón por la cual ha aumentado el desarrollo de malware para este tipo de dispositivos, especialmente en aquellos dispositivos que utilizan plataformas de código abierto, ya que estas utilizan interfaces simples y han penetrado en gran medida el mercado.

En esta medida, para contrarrestar las amenazas descritas es importante tener en cuenta que aunque la regulación[92] ya estableció las condiciones para la homologación de equipos terminales en Colombia, dichas condiciones tienen en cuenta normas técnicas y requisitos enfocados principalmente en garantizar el cumplimiento de especificaciones que eviten la interferencia con otros dispositivos y cumplan con límites de exposición humana a campos electromagnéticos; sin embrago hasta la fecha no se han contemplado condiciones y/o requisitos adicionales que puedan tenerse en cuenta respecto a la seguridad "mínima" que deben tener los dispositivos, para proteger la información almacenada por los usuarios en estos.

Considerando las facultades que tiene la CRC para establecer las condiciones y requisitos para la homologación de equipos terminales, y siendo conscientes de las vulnerabilidades existentes en los dispositivos móviles, en los que se almacena información de carácter privado de los usuarios de servicios de telecomunicaciones, resulta apropiado que esta Comisión adelante las siguientes actividades:

1. Evaluar las medidas mínimas técnicas de seguridad que deberían ofrecer los dispositivos que se utilizan en las redes de telecomunicaciones y los equipos terminales móviles que se usan en las redes de los PRST de Colombia, dispositivos como Access Point, Equipos terminales móviles, switches, routers y equipos con conectividad Wi-Fi.

2. Realizar un estudio del tipo de dispositivos disponibles en Colombia que cumplen con cada uno de los diferentes recursos disponibles para cubrir las vulnerabilidades identificadas en los dispositivos de red.

## 7.3 PROCEDIMIENTOS PARA LA INVESTIGACIÓN DE DELITOS INFORMÁTICOS/ PRESERVACIÓN DE EVIDENCIA DIGITAL

En la actualidad el Ministerio de Defensa en conjunto con el Ministerio de Justicia, Ministerio TIC y el DNP está adelantando la estructuración de un nuevo Conpes que recoja los lineamientos planteados en el Conpes 3701 de 2011, aún vigente pero con gran parte de las actividades definidas para cada una de las entidades estatales ya cumplidas; es por esto que se requieren nuevos parámetros y responsabilidades para el fortalecimiento de la Estrategia Nacional de Ciberseguridad y Ciberdefensa, de acuerdo al gran crecimiento en torno a las TIC, y en consecuencia de los ataques cibernéticos.

[92] Capítulo I del Título XIII de la Resolución CRC 087 de 1997,

En este aspecto se hace necesario un trabajo permanente y coordinado entre todas las Entidades de orden nacional con injerencia en la actualización de la estrategia. Es así como el rol de la CRC está enfocado en gran medida en adelantar y participar en mesas de trabajo con otras entidades del Gobierno Nacional a fin de brindar el acompañamiento requerido dada su calidad de organismo técnico del sector TIC; y de otra parte, a realizar las adecuaciones regulatorias que sean pertinentes para contribuir a la consolidación de la estrategia nacional, desde el ámbito de sus competencias de regulación de redes y protección de los derechos de los usuarios TIC. En este sentido se considera necesario que la CRC forme parte directa del comité interinstitucional a cargo de las labores de actualización del CONPES 3701.

De otro lado, la CRC adelantó en el 2014 actividades con el Ministerio de Defensa y particularmente con el Comando Conjunto Cibernético – CCOC mediante la realización de mesas de trabajo con el fin de analizar y definir con las demás entidades y la industria, las infraestructuras críticas del país de todos los sectores, se propone durante el año 2015 continuar con la realización de dichas mesas de trabajo lideradas por el CCOC mediante un comité participativo con las demás entidades de gobierno, que permitan diseñar medidas efectivas para proteger las infraestructuras criticas del país. Es de precisar, que para el caso particular de la definición de infraestructuras criticas del sector TIC, la mesa se encuentra liderada por el Ministerio de TIC con la coordinación de la dirección de Estándares y Arquitectura de TI.

En lo relativo a la identificación de Infraestructuras Críticas, esta es una tarea en cabeza del Comando Conjunto Cibernético del Ministerio de Defensa. Para dicha identificación se han establecido metas específicas, que van desde el establecimiento de una red de contactos, hasta el diseño, desarrollo y consolidación de guías a través de las cuales se definan lineamientos generales que permitan contar con procedimientos comunes para mejorar la seguridad de los sistemas informáticos asociados incluyendo la infraestructura de las telecomunicaciones. Las guías han sido divididas en 5 categorías diferentes que comprenden la Gestión de Activos, Gestión de Vulnerabilidades, Gestión de Riesgos, Gestión de Incidentes de Seguridad y Gestión de Continuidad del Negocio, las cuales serán implementadas a manera de piloto a lo largo del año 2015.

Es importante aclarar que dicha identificación no se limita al sector de telecomunicaciones y TIC, sino que considera sectores como petroquímico, hídrico, minero, educativo y alimentos, entre otros. El ejercicio de identificación de infraestructuras críticas ha desarrollado un análisis de las experiencias internacionales, considerando países como en Israel, Estados Unidos, Canadá, Reino Unido, España, Chile y Australia.

Por otro lado, se identificaron una serie de actividades que la CRC podrá adelantar con las demás Entidades del estado competentes para lograr un marco de Ciberseguridad con mayor alcance; dentro de las actividades propuestas se recomienda:

1. Fomentar espacios de trabajo y colaboración con el Comité Consultivo Permanente I – CCP.I de CITEL, que trata temas relacionados a investigación sobre fraudes y prácticas antirreglamentarias, y facilitar el intercambio de datos a nivel internacional respecto a incidentes de Ciberseguridad.
2. Llevar a cabo mesas de trabajo con PRST, el CCOC y la CRC, para definir un modelo de esquemas tecnológico y de procesos en los que se reporten incidentes de Ciberseguridad al CCOC para su correspondiente análisis, tratamiento y acción de respuesta frente a eventuales amenazas.

## 8. CONSULTA PÚBLICA

De lo anterior, se evidencia que se requiere definir una estrategia específica en la cual se establezcan metas y responsabilidades teniendo en cuenta las competencias de cada una de las Entidades del gobierno, para de esta forma poder apoyar al máximo la definición y ejecución de la nueva Estrategia Nacional de Ciberseguridad y Ciberdefensa.

Mediante este documento la CRC presenta el trabajo de investigación desarrollado y plantea las temáticas de acción que pueden llegar a ser adelantadas por el regulador o por otras Entidades para aumentar los niveles de seguridad cibernética en el país teniendo como línea base las buenas practicas adoptadas por otros países y la cooperación que mantiene con organismos internacionales como la OEA, UIT, OECD entre otros.

Por lo tanto, se invita al sector a presentar sus aportes a partir de las temáticas expuestas en los capítulos 7 y 8 del presente documento a saber:

1. Seguridad de Redes
2. Protección de Datos del Usuario
3. Procedimientos para la investigación de delitos informáticos/ Preservación de evidencia digital

Y adicionalmente sobre los siguientes cuestionamientos generales:

1. ¿Cómo considera que la CRC debe reforzar la regulación actual en materia de seguridad de las redes de los PRST en Colombia, a efectos de aumentar los niveles de protección a usuarios finales?
2. ¿Qué aspectos técnicos y procedimientos deberá tener en cuenta la CRC para promover la protección de los equipos utilizados para conectarse a las redes de telecomunicaciones?
3. ¿De qué manera considera que la CRC puede lograr que los agentes del sector cumplan con los estándares de Ciberseguridad establecidos en la regulación vigente y que procedimientos adicionales o medidas se deberán tener en cuenta?
4. ¿Considera necesario que se adelante un estudio específico sobre temas relacionados a computación en la nube con el fin de garantizar la privacidad y seguridad de la información de los usuarios de este servicio en el territorio nacional?
5. ¿Qué tareas conjuntas puede adelantar el sector TIC para fomentar el aumento de la cultura de Ciberseguridad en los usuarios de Telecomunicaciones?

## 9. FUENTES DE INFORMACIÓN


- Gobierno de España, Presidencia del Gobierno. Estrategia de Ciberseguridad Nacional. 2013 https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ES_NCSS.pdf

- Tendencia de Seguridad Cibernética en América Latina y el Caribe, Ornagizacion de los Estados Americanos – Symantec, 2014. Consultado en: http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

- Fundación ESYS, Estudios sobre la necesidad de certificación y acreditación en materia de Ciberseguridad.. Madrid Noviembre 2013. http://www.fundacionesys.com/files/Estudio%20ESYS_Ciberseguridad.pdf

- Jaider Ospina Navas. "Un acercamiento al estado del arte en Cloud Computing". Universidad Distrital Francisco José de Caldas. Bogotá. Julio, 2013.http://comunidad.udistrital.edu.co/revistavinculos/files/2013/09/Un-acercamiento-al-estado-del-arte-en-Cloud-Computing.pdf

- Wegener Henning ,La Ciberseguridad en la Unión Europea.. 14 de Julio de 2014. http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO77bis-2014_CiberseguridadProteccionInformacion_H.Wegener.pdf

- Iniciativa Ley convergente. México. http://www.presidencia.gob.mx/wp-content/uploads/2014/03/INICIATIVA-LEY-CONVERGENTE.pdf Marzo de 2014.

- Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006. "Sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE".

- Ley 25 de 2007, de 18 de octubre, de conservación de datos relativos a la comunicaciones electrónicas y a las redes públicas de comunicaciones. España.

- Estrategia de Ciberseguridad de Nacional de España. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ES_NCSS.pdf, 2013.

- Consejo de Europa. Convenio sobre la Ciberdelincuencia. Budapest 23 de noviembre de 2001. Disponible en: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF.

- Departamento Nacional de Planeación. Consejo Nacional de Política Económica y Social. Documento CONPES 3701 de 2011. Disponible en: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf.

- Michael G. Noblett, Mark M. Pollitt, Recovering and Examining Computer Forensic Evidence, (2000) htt://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2000/computer.html

- Unión Internacional de Telecomunicaciones – UIT, Recomendación UIT-T X.1205 Aspectos generales de la ciberseguridad. 2008 Disponible en: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-S&type=items

- Rafael García del Poyo, CLOUD COMPUTING: Aspectos jurídicos clave para la contratación de estos servicios; Extraído de Short Link: http://tinyurl.com/pd92qn8

- INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE

- McDowell M. 2009. Security Tip (ST04-015 ) Understanding Denial-of-Service Attacks, US CERT United States Computer Emergency Readiness Team. Consultado de: https://www.us-cert.gov/ncas/tips/ST04-015

- The National Cyber Bureau Israel, Consultado en : http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/default.aspx