LOS NUEVOS RETOS EN MATERIA DE CIBER-SEGURIDAD EN COLOMBIA

LINA MARÍA MORENO PÉREZ

TUTOR

ÁLVARO MÉNDEZ CORTES

MAGISTER EN EDUCACÍON

UNIVERSIDAD MILITAR NUEVA GRANADA

FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD

DIPLOMADO EN GERENCIA DE LA SEGURIDAD

BOGOTÁ D.C. 2018

Resumen

En el mundo actual la información fluye en gran medida a través de medios electrónicos y ellos pueden ser vulnerados en cualquiera de los momentos en que es compartida.

El documento abordara el conocimiento de los nuevos retos a los cuales se enfrenta Colombia en cuanto al tema de la Ciber seguridad donde todos los días el individuo está expuesto a enfrentar diferentes amenazas, por una parte se estudiara el concepto y la evolución que ha tenido este tema en el contexto colombiano, adicional a ello conocer las principales normales legales que se encuentran en vigencia, y en última instancia proponer una estrategia para enfrentar estos nuevos retos.

Palabras Clave: Ciberseguridad, Seguridad, Retos

Abstract

In today's world, information flows to a large extent through electronic means and they can be violated at any time when it is shared

The document will address the knowledge of the new challenges faced by Colombia regarding the issue of cyber security where every day the individual is exposed to face different threats, on the one hand the concept and evolution that this topic in the Colombian context, in addition to knowing the main legal normals that are in force, and ultimately propose a strategy to face these new challenges

Keywords: Cybersecurity , Security , Challenges

Glosario

Bots Computadora en la cual, un virus o gusano, ha instalado programas que se ejecutan automáticamente, Permiten al atacante acceso y control.

Bot Network Colección de máquinas infectadas, comprometidas semanas o meses antes por los atacantes**,** Se usan para lanzar ataques simultáneos.

Bundling Pega virus o spyware a descargas que hace el usuario Cuando el usuario instala el software descargado, también instala el programa del atacante.

Delito informático: El delito informático puede comprender tanto aquellas conductas que valiéndose de medios informáticos lesionan intereses protegidos como la intimidad, el patrimonio económico, la fe pública, la seguridad, etc., como aquellas que recaen sobre herramientas informáticas propiamente dichas tales como programas, computadoras, etc.

Enumeration: Uso de herramientas para obtener la información detallada (servicios ejecutándose, cuentas de usuario, miembros de un dominio, políticas de cuentas, etc.) sobre un sistema remoto, con el intento de atacar la seguridad de cuentas y servicios en el objetivo**.**

Footprinting: El uso de herramientas y de la información para crear un perfil completo de la postura de la seguridad de una organización.

Gaining Access: Hay varias herramientas disponibles que pueden permitir a un hacker tomar control de un sistema. Por ejemplo, Samdump y Brutus son crackers de passwords. Samdump se utiliza extraer los passwords de los archivos. Brutus es un cracker de password remoto. Si un hacker consigue el acceso a una copia de una base de datos, el hacker podría utilizar l0phtcrack y extraer los usuarios y passwords exactos.

Keylogging Programa que captura y registra los teclados del usuario Después accede o envía secretamente los datos al atacante.

Negación de Servicio Ataque diseñado específicamente para evitar el funcionamiento normal de una red o sistema y evitar el acceso de usuarios autorizados.

Packet Sniffer Programa de software que monitorea el tráfico de red Usados para capturar y analizar datos, especialmente passwords.

Port Redirection Después que el atacante tiene identificado y accede al tráfico del firewall que puede permitir tráfico de entrada de un puerto origen 53, procurar instalar un software Port Redirector en el equipo dentro del firewall. El Port Redirector tomará el tráfico entrante destinado para un puerto (53) y lo enviará a otro equipo detrás del firewall en otro puerto (3389).

Privilege Escalation Un hacker puede causar la mayoría del daño consiguiendo privilegios administrativos en una red. Hay varias utilidades que un hacker puede utilizar para ganar privilegio administrativo. Por ejemplo, la utilidad Getadmin.exe es usada para otorgar a usuarios comunes privilegios administrativos agregando a estos usuarios al grupo de administradores. Esta utilidad funciona con todas las cuentas excepto con la cuenta de Guest.

Remote Admistration Tools Eso permite que un usuario remoto realice cualquier acción remotamente vía un puerto a su elección sin un usuario local del sistema que lo habilite.

Rootkit Conjunto de herramientas usadas por el atacante después de infiltrar una computadora Los hay disponibles para la mayoría de S.O.

Le permiten:

- Mantener el acceso
- Evitar detección (oculta proceso y archivos)
- Construir backdoors ocultas
- Obtener información de la computadora comprometida y de los otras computadoras en la red

Scanning: El atacante usa herramientas y la información obtenida para determinar qué sistemas están vivos y accesibles desde Internet así como qué puertos están escuchando en el sistema.

Spyware Software que obtiene información sin el conocimiento del usuario. Típicamente viene adherido con otro programa (legítimo) El usuario desconoce que al instalar uno instala el otro Monitorea la actividad del usuario en la red y retransmite esa información al atacante Captura y mantiene: direcciones de correo, passwords, números de tarjetas de crédito, información confidencial, etc.

Scripts Programas o listas de comandos, disponibles como shareware en sitios de hackers Pueden copiarse e insertarse remotamente en una computadora Usados para atacar y quebrantar la operación normal de una computadora.

Troyano Programa malicioso inadvertidamente descargado e instalado por el usuario Algunos pretenden ser aplicaciones benignas Muchos se ocultan en la memoria de la máquina con nombres no descriptivos Contiene comandos que la computadora ejecuta automáticamente sin conocimiento del usuario Algunas veces actúan como zombies y envían spam o participan en un

ataque de negación de servicio distribuido Pueden ser un Keylogger u otro programa de monitoreo que colecciona datos que envía encubiertamente al atacante Muchos troyanos ahora intentan deshabilitar los programas antivirus

Worms Viajan a través de las redes, Se duplican a sí mismos y se auto envían a direcciones que están en la computadora host**,** Se propagan enviando copias de sí mismos a otras computadoras por e-mail o por Internet Relay Chat (IRC)

Virus Programa o pieza de código que se difunde de computadora a computadora sin consentimiento del usuario Causan eventos inesperados y negativos cuando se ejecutan en la computadora Contaminan programas legítimos Son introducidos a través de anexos en e-mails Usan nombres ingeniosos para atraer la curiosidad del lector

Introducción

En el mundo se han presentado avances en cuanto al tema de la tecnología, para nadie es un secreto que la globalización en este tema es uno de los que continuamente evoluciona y está a la vanguardia convirtiéndose en un tema preponderante de conocimiento.

Para entender sobre el tema de la ciberseguridad hay que tener en cuenta el término cibercultura, este, según el artículo "cibercultura y las nuevas nociones de privacidad" publicado por María Belén Albornoz "es el conjunto de sistema socio técnico cultural que tienen lugar en el ciberespacio".

La sociedad utiliza los recursos tecnológicos en su beneficio o interés, y puede recurrir a este de una manera tanto asertiva como negativa según la percepción de cada individuo, cabe señalar que la misma tecnología dado su avance esta presente en la actividades diarias y sin duda alguna afecta el desarrollo personal o particular dado que incluso ha llegado a suplantar multiples escenarios de la cotidianidad.

Los avances de la ciencia y la tecnología han llevado a replantear muchos de los escenarios que se muestran en el sistema internacional como en el sistema nacional colombiano, la economía, las relaciones internacionales, la cultura, el deporte y la ciencia entre otros han sido tocados por estos desarrollos relacionados con la cultura ciber.

Se pretende resaltar los nuevos retos a los cuales se enfrenta el sistema nacional colombiano frente a los temas de la ciberseguridad y que posibles medidas de seguridad se pueden tomar ante la amenaza que directa o indirectamente afecta la sociedad en el diario vivir.

Antecedentes en Colombia frente al tema de la ciberseguridad

Según ISACA (Information Systems Audit and Control Association) ciberseguridad es "La protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados" por lo tanto, esta tiene como foco de atención proteger la información digital que "vive" en los sistemas interconectados. En consecuencia, está comprendida o pude conciliarse como una rama dentro de la seguridad de la información.

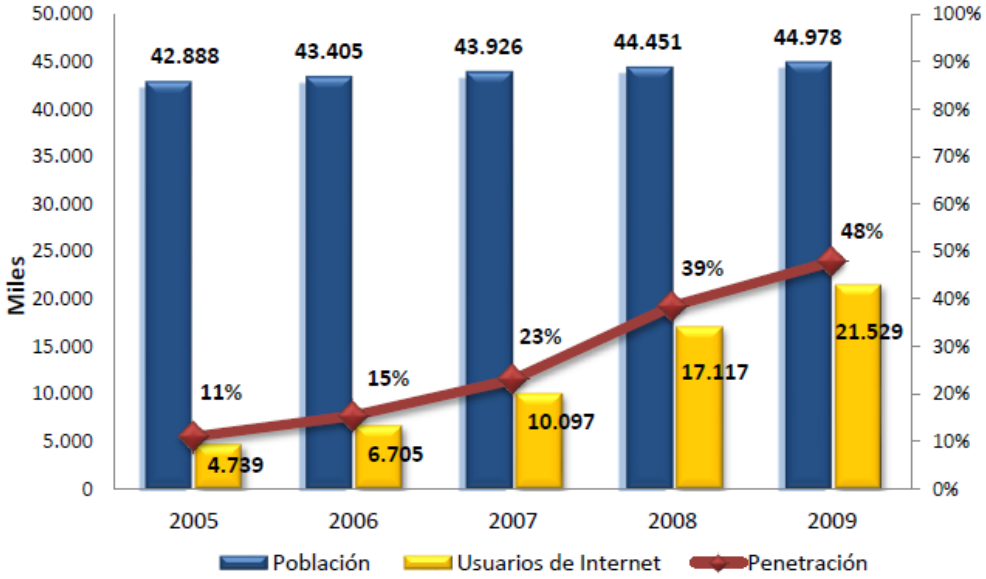
La seguridad de la información por ISACA (Information Systems Audit and Control Association) "sustenta de metodologías, normas, técnicas, herramientas, estructuras organizacionales, tecnología y otros elementos, que soportan la idea de protección en las distintas facetas de la información, aplica y gestiona medidas de seguridad apropiadas, a través de un enfoque holístico."

Entonces teniendo en cuenta las definiciones anteriores se puede inferir que la ciber seguridad hace una orientación a la protección de los datos digitales que circulan por la red y a los elementos que van entrelazados y que trasmiten o procesan algún tipo de datos, y la seguridad de la información hace un enfoque hacia resguardar los medios a través de los cuales fluye la información de cualquier peligro que puedan afectarla.

Teniendo claras las definiciones se analizará cuáles fueron los antecedentes frente al tema de la ciber seguridad en el Estado colombiano, en primera medida hay que resaltar que en el país el desarrollo de los sistemas de comunicación a través del ciberespacio entre los años 2005 y 2009

tuvo un amplio desarrollo presentándose un número elevado de usuarios que accedió al uso de internet como se puede apreciar en la siguiente grafica

Grafica N° 1: Usuarios a Internet 2005- 2009



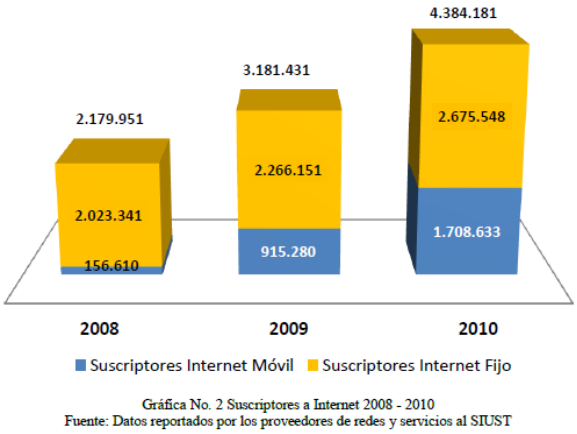
Gráfica No. 1 Usuarios a Internet 2005 - 2009
Fuente: Datos reportados por los proveedores de redes y servicios al SIUST, DANE

Fuente: Tomado de los datos reportados por los proveedores de redes y servicios al SIUST, DANE.

La gráfica reporta los usuarios con acceso a internet del periodo comprendido entre 2005 y 2009, está es importante porque estadísticamente demuestra en millones de personas como fue el incremento y aumento significativo del uso de la internet.

En segunda medida entre los años del 2008 y 2010 se extendió el uso del internet alcanzando un total de 4.384.181 suscriptores de servicio fijo y móvil. De estos, el 39% corresponde a suscriptores fijos y el 61% a usuarios móviles, como se aprecia en la gráfica No 2

Grafica N° 2: Suscriptores a Internet 2008-2010



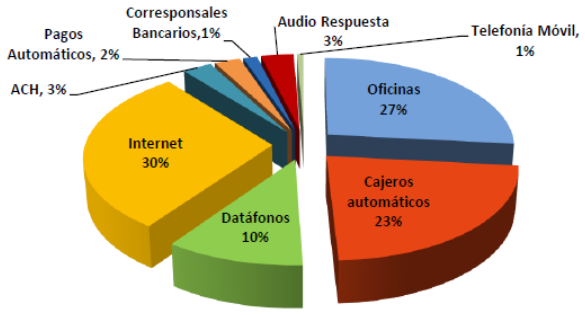
Gráfica No. 2 Suscriptores a Internet 2008 - 2010
Fuente: Datos reportados por los proveedores de redes y servicios al SIUST

Fuente: Tomado de los Datos reportados por los proveedores de redes y servicios al SIUST

Por lo tanto se puede concluir con los datos estadísticos de la gráfica No 2 que el uso del internet fijo tuvo una preponderancia frente al internet móvil, y que la población estaba haciendo más uso de las tecnologías fuera de su casa, que dentro de ella.

Para el año 2010 la superintendencia financiera de Colombia reporto que un 30% de las transacciones monetarias y no monetarias fueron ejecutadas vía internet, esto refleja un incremento del 12% en el número de operaciones realizadas por este canal, respecto al año 2008, como lo muestra la gráfica No.3.

Grafica N° 3: Operaciones Monetarias y no monetarias por canal 2010



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

Fuente: Tomado del informe de transacciones y operaciones superintendencia financiera de Colombia.

En el año 2010 hay avances importantes en el uso del internet móvil para la realización de transacciones dentro de la población y este mismo escenario ayudo para que las personas pudieran ser más eficientes y a un solo “click” realizaran cualquier operación bancaria con un mínimo de espera y un máximo de eficiencia facilitando el trámite bancario.

Para el primer trimestre del año 2011 se tuvo un caso de ataque de seguridad cibernética ejecutado por Anonymous , atacando portales de la Presidencia de la República, Senado de la República, Gobierno en línea y los Ministerios del Interior y Justicia, Cultura y Defensa, dejando fuera de servicio sus páginas web por varias horas.

Este ataque se generó como mecanismo de protesta por la presentación de un proyecto de Ley denominado “Ley Lleras” presentado en abril del 2011 a través del cual se pretendía generar un nuevo estatuto de control al espectro electromagnético , entre otros pretendía regular la responsabilidad por las infracciones a los derechos de autor y al derecho a la conexión a internet.

Cabe resaltar que este grupo también ha realizado ataques a entidades internacionales públicas como privadas, entre las cuales están PayPal, el Banco Suizo Post Finance, MasterCard, y Visa.

Aunado lo anterior pero no menos importante es lo relacionado con la Ley 1273/09 que trata de los nuevos modelos penales que se crearon relacionados con los delitos informáticos y la protección de la información y de los datos.

Las denuncias que fueron reportadas por los ciudadanos ante la Policía Nacional desde enero hasta diciembre del 2009 indican que se atendieron 575 delitos informáticos, entre este número 259 de estas fueron por acceso abusivo a un sistema informático, 247 fueron por hurto de medios electrónicos, 17 por intercesión de datos informáticos, 35 por la violación de datos personales, 8 por la transferencia no consentida de activos , 5 por el daño informático, 3 por la obstaculización ilegitima de un sistema informático. También para el año 2010 la cantidad de delitos aumento en un 73% al alcanzar un total de 995 delitos informáticos.

Normas legales que rigen en materia de Ciberseguridad en Colombia.

Sobre las normas legales que rigen a Colombia en Ciberseguridad, se tomara en cuenta el marco internacional y después el Nacional

Marco Internacional

En el tema las diferentes naciones se han agrupado y diseñado esquemas y propuestas del cómo afrontar los retos del ciber delito y las medidas de ciberseguridad, el siguiente cuadro muestra algunas de esas decisiones de carácter internacional a las cuales Colombia se ha acogido.

Tabla N°.1 Normas Internacionales

Instrumento	Materia
Directiva 2006/24 de la Unión Europea	Se establece 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.
Pronunciamientos de Principios	Resoluciones UNGA: 55/63 y 56/121 sobre la lucha contra el 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). 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).
Marco de trabajo de estrategias nacionales de ciberseguridad. Manual de la OTAN	LA OTAN publica en el año 2012 en colaboración con la NATO Cooperative Cyber Defence Centre of Excellence el manual para la formulación de estrategias nacional de ciberseguridad para sus países miembros.
Declaración de la Cumbre de Gales de la OTAN en 2014	Documento oficial de los resultados de la Cumbre de la OTAN celebrada en Cardiff (Gales) los días 4 y 5 de septiembre de 2014, en donde se resaltan acuerdos para abordar la ciberseguridad en los países de dicha alianza.
Declaración sobre la protección de infraestructura crítica ante las amenazas emergentes (Aprobado durante la quinta sesión plenaria, celebrada el 20 de marzo de 2015)	Declaración en donde, entre otros, la Secretaría Ejecutiva del CICTE de la OEA desarrolla un proyecto de asistencia técnica que, permita a estos la elaboración de un listado de su infraestructura crítica y su clasificación, basados en sus respectivos activos, sistemas, redes y funciones esenciales, para hacer posible la mejor evaluación de vulnerabilidades, brechas, amenazas, riesgos e interdependencia.
Declaración sobre Seguridad en las Américas de la OEA (México, 2003)	Identifica como relevantes, entre otras nuevas amenazas, el terrorismo y los ataques a la seguridad cibernética, y comprometió a los Estados miembros a desarrollar una cultura de seguridad cibernética en las Américas con la adopción de medidas de prevención eficaces para prever, enfrentar y responder a los ataques cibernéticos, cualquiera fuera su origen, luchando contra las amenazas y la delincuencia cibernética, tipificando los ataques contra el espacio cibernético, protegiendo la infraestructura crítica y asegurando las redes de los sistemas.

Fuente: Tomado del CONPES 3854, normativa de ciberseguridad en Colombia

Es evidente que el sistema internacional muestra preocupación por generar diversas alternativas de control y seguridad frente al riesgo de ser afectados no solo los Estados sino las empresas por un delito que evoluciona día a día y al cual hay que hacerle frente de manera sistemática y mancomunada.

Marco Nacional

El Estado colombiano también ha diseñado esquemas y propuestas del cómo afrontar los retos del ciber delito y las medidas de ciberseguridad, el siguiente cuadro muestra algunas de esas decisiones de carácter internacional a las cuales Colombia se ha acogido.

Tabla N°. 2 Normas Nacionales

Norma	Contenido
Constitución Política de Colombia	Artículos 11, 12, 13, 14, 17, 21, 22, 24, 29, 44, entre otros. Por ejemplo, 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. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
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. Se tratan conceptos como: mensaje de datos (artículos 2º y 5º), el principio de equivalencia funcional (artículos 6º, 8º, 7º, 28º, 12º y 13º), la autenticación electrónica (artículo 17º), la firma electrónica simple (artículo 7º), la firma digital (artículo 28º), y la firma electrónica certificada (artículo 30º, modificado por el artículo 161 del Decreto Ley 019 de 2012).
Ley 594 de 2000 (Ley General de Archivos)	Habilita el uso de nuevas tecnologías de manera general, es posible establecer que para satisfacer los requerimientos establecidos en esta norma sea viable usar firmas electrónicas simples, certificadas y firmas digitales.
Ley 599 de 2000 (Código Penal)	Por la cual se expide el código penal colombiano.
Ley 600 de 2000 (Código de Procedimiento Penal)	Por la cual se expide el código de procedimiento penal.
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 Ministerio de Tecnologías de la Información y las Comunicaciones- , 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.
Ley 906 de 2004 (Código de Procedimiento Penal)	Por la cual se expide el código de procedimiento penal (corregida de conformidad con el Decreto 2770 de 2004)
Ley 962 de 2005 (racionalización de trámites y procedimientos)	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Prevé el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados.
Ley 1032 de 2006 (derechos de autor y conexos)	Por la cual se modifican los artículos 257, 271, 272 y 306 del código penal (artículo 271. violación a los derechos patrimoniales de autor y derechos conexos).

Fuente: Tomado del CONPES 3854, normativa de ciberseguridad en Colombia

Es evidente que en el Sistema nacional muestra preocupación por generar diversas alternativas de control y seguridad frente al riesgo de ser afectados no solo al Estado sino las empresas por un delito que evoluciona día a día y al cual hay que hacerle frente de manera sistemática.

Los nuevos retos en la Ciberseguridad en Colombia

Marco Internacional

Frente al tema las diferentes naciones han implementado diferentes esquemas y propuestas del cómo afrontar los retos del ciber delito y las medidas de ciberseguridad, el siguiente cuadro muestra algunas de esas decisiones de carácter internacional a las cuales Colombia se ha acogido.

Tabla N° 3

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

Fuente: Tomado CONPES 3701, Lineamientos de política para ciberseguridad, ciberdefensa

Es evidente que el sistema internacional muestra preocupación por generar nuevos retos para la ciberseguridad de control y seguridad frente al riesgo de ser afectados no solo los Estados sino las empresas por un delito que evoluciona día a día y al cual hay que hacerle frente de manera sistemática y mancomunada.

Marco Nacional

En el sistema Nacional Colombiano se ha fomentado diferentes iniciativas en algunos sectores uno de estos es el Modelo de la seguridad de la información para la estrategia de un gobierno en línea el cual la entidad encargada de este modelo ha sido el Ministerio de las Tecnologías de Información y las Telecomunicaciones, la finalidad de este modelo de seguridad hace referencia a un conjunto de políticas que quieren garantizar la protección de información de cada individuo y una alta confiabilidad en el gobierno en línea con tres pilares estratégicos que son: "tener la disponibilidad de la información y los servicios , el segundo la integridad de la información de los datos y la tercera la confidencialidad de la información."

Al sistema colombiano dentro de sus iniciativas para la seguridad de las telecomunicaciones se le han hecho diferentes recomendaciones dentro de las cuales la más importante ha sido para la entidad líder la comisión de regulación de telecomunicaciones la cual trata sobre crear una estrategia a nivel nacional de ciberseguridad que implemente el desarrollo de marcos jurídicos más exactamente frente al tema de la ciberseguridad que sean congruentes frente a los parámetros internacionales anteriormente mencionados también da la recomendación de la elaboración de sistemas que den una respuesta inmediata a incidentes en materia de

ciberseguridad y propone fomentar una cultura nacional de ciberseguridad que mejore los niveles de protección de la infraestructura crítica de la información en Colombia.

El centro de Centro de coordinación de atención a incidentes de Seguridad Informática Colombiano para proveedores de servicios de Internet (CSIRT) con la cámara colombiana de informática y telecomunicaciones (CCIT) fomentaron la coordinación para atender incidentes de la seguridad informática el cual es manejado contactando directamente con los centros de seguridad de las más grandes empresas proveedoras de Internet en Colombia y está tiene que tener la suficiente capacidad de coordinar y solucionar las preocupaciones y acusaciones sobre problemas de seguridad informática que sean recibidas.

Desde el año 2007 se ha venido fomentando en Colombia la importancia de generar una política de ciberseguridad y ciberdefensa, para esta socialización el Estado colombiano se ha apoyado en la organización de estados americanos (OEA) por medio del comité interamericano contra el terrorismo (CICTE) con la ayuda de ellos para el año 2008 se realizó una jornada de concientización sobre la seguridad cibernética y en octubre del 2009 se hizo una mesa de diálogo nacional las conclusiones frente a estas actividades fueron que el Ministerio de Defensa Nacional debería tener más responsabilidad en estos temas y estar involucrado con referente a la seguridad cibernética .

También en materia de ciberseguridad para el año 2010 este tema fue incluido en el plan nacional de desarrollo "Prosperidad para Todos" del entonces presidente Juan Manuel Santos con el nombre de Plan vive digital que fue liderado por el Ministerio de Tecnologías de la Información y las Comunicaciones.

Para el año 2011 el gobierno nacional colombiano creo el COLCERT que está formado hasta la fecha de hoy por personal civil y militar y la principal función que tiene es "coordinar las acciones necesarias para proteger la infraestructura del Estado frente a momentos de emergencia de Ciberseguridad que transgreden la seguridad nacional."(Osorio, 2018), también se creó el

Comando Conjunto Cibernético de las Fuerzas Militares para resguardar la defensa cibernética del Estado Colombiano y también en defender la información militar en el Ejército, Fuerza Aérea y Armada Nacional.

Se creó el Centro Cibernético Policial que se hace responsable de la investigación, prevención y apoyo en los delitos informáticos, cuenta con un comando de Atención Inmediata Virtual (CAI VIRTUAL) para que los ciudadanos puedan hacer denuncias.

Figura N° 1: Modelo de coordinacion Intersectorial

Fuente: Tomada del CONPES 3701-Ministerio de Defensa

El Centro Cibernético Policial y el COLCERT trabajan de una manera conjunta, ya que utilizan información para asemejar perfiles de integrantes no reconocidos y el Centro Cibernético Policial brinda el debido apoyo en temas de investigación digital y judicial, esto para que se interconecten y estén involucrados en temas de ciberseguridad en las entidades del Estado y del sector privado. Esta incentiva al Estado colombiano a dar apoyo en otros países de

América Latina, de igual manera se ha podido recibir ayuda de las Organizaciones de los Estados Americanos (OEA) por medio del Comité Interamericano contra el Terrorismo (CICTE), como fue mencionado anteriormente.

Hay que tener en cuenta que todos estos esfuerzos hechos por el Estado Colombiano en el año 2014 fueron puestos en duda porque Colombia fue atacada en cuanto a la parte de Ciberseguridad con el caso de las intercepciones Andrómeda y el rastreo de algunos correos electrónicos, eso sin duda alguna obligo a Colombia a formalizar y doblegar la Comisión Digital, que obedecía de la Agencia Nacional de Seguridad Cibernética, estas dos tuvieron que trabajar tanto en Fuerzas públicas como privadas y tuvieron que crear nuevas políticas para la ciberseguridad y la ciberdefensa colombiana y esto mismo ayudo a implementar acuerdos internacionales para así mejorar la seguridad informática.

En marzo del año 2014, países pertenecientes a la Organización de Estados Americanos (OEA) tales como Canadá, Estados Unidos, Reino Unido entre otros analizaron los temas de ciberseguridad para Colombia y concluyeron que el país en cuanto a la seguridad digital necesitaba tener un lineamiento más específico.

Del 2015 hasta ahora en Colombia se han incrementado el uso masivo de las tecnologías de la información y las comunicaciones (TIC) ya que se ve una masificación de redes sociales , incremento en los servicios en línea , incremento en economía digital y las nuevas y sofisticadas formas del crimen digital.

Tabla N° 4 Proyección de algunos indicadores de uso de Tic a nivel global

Proyecciones	2015	2020	Incremento porcentual
Más usuarios de banda ancha móvil	3 mil millones	4 mil millones	33%
Más terminales conectados	16,3 mil millones	24,4 mil millones	49%
Más datos generados	8,8 zettabytes	44 zettabytes	400%
Más tráfico IP de red (mensual)	72,4 exabytes	168 exabytes	132%
Dispositivos (Internet de las cosas)	15 mil millones	200 mil millones[a]	1200%
Tamaño del mercado de la nube pública global	USD 97 mil millones	USD 159 mil millones	63%

Fuente: Tomada del CONPES 3854

En la tabla N°4 se puede evidenciar las propuestas la creciente relevancia del entorno digital sobre las actividades socioeconómicas, y su alto dinamismo, ha traído consigo un conjunto de incertidumbres, riesgos, amenazas, vulnerabilidades e incidentes.

Por esto el país adopto fortalecer sus capacidades para prevenir y mitigar los riesgos en cuando a su seguridad informática para así poder tener un crecimiento en la economía digital nacional lo cual ayuda a promover una mayor economía y social en Colombia. Para todo esto se gestionó los principales pilares que se encuentra en el Conpes 3854 del año 2016 que cuenta con 5 pilares fundamentales que son:

1. Establecer un marco institucional claro en torno a la seguridad digital, basado en la gestión de riesgos.
2. Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital.
3. Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos.
4. Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos.

5. Impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional.

Colombia para ejecutar este plan de acción se propuso un periodo de 3 años (2016-2019), en el cual invertirá 85.070 millones de pesos y las entidades principales en direccionar este plan de acción serán en primera instancia el Ministerio de las Tecnologías de la información y la comunicación , seguido del Departamento Nacional de Planeación y la Dirección Nacional de Inteligencia.

Según el informe de la Política Nacional de Seguridad Digital se estima que si esa implementación resulta acertada, Colombia tiene presupuestado que si el plan de acción resulta de manera acertada el empleo aumentara en 307000 para el año 2020 y esto incrementa el producto interno bruto de la economía en un 0.1%.

Estrategia para enfrentar los nuevos retos en la ciberseguridad Colombiana

A lo largo de la investigación se ha visto que el ciberespacio sin duda alguna ocupa todas las infraestructuras de información accesibles a través del internet y que traspasa cualquier límite territorial, en la actualidad se ha incrementado el uso del internet ya sea para hacer una trasferencia bancaria vía internet o simplemente para el uso de redes sociales y estar más conectados con los demás, de alguna manera esto tiene un grado de vulnerabilidad porque en los últimos años los ataques en las infraestructuras son más frecuentes y complejos, mientras que al mismo tiempo los delincuentes se han vuelto más profesionales. Y estos mismos utilizan el ciberespacio como un lugar para sus actividades.

El gobierno colombiano aspira hacer una gran contribución en materia de la seguridad digital y el ciberespacio promoviendo una mejor economía, y una mejor prosperidad social, la seguridad digital en Colombia debe garantizar a un nivel que esté acorde con la importancia y protección

que exigen las infraestructuras de información interconectadas sin obstaculizar las oportunidades y la utilización del ciberespacio. En este contexto, el nivel de seguridad cibernética debe alcanzar la suma de todos los fondos nacionales e internacionales de las medidas tomadas para proteger la información y las comunicaciones.

La seguridad cibernética debe basarse en un enfoque integral que requiera incluso el intercambio de información y coordinación más intensivos. Está se debe centrar en enfoques y medidas civiles para así poder proteger sus capacidades y medidas basadas sobre los mandatos para hacer de ella una parte de la seguridad preventiva en Colombia.

Dada la naturaleza global de la tecnología de la información y las comunicaciones, los aspectos de política son indispensables, y también dentro del marco de estas políticas se implementaría la cooperación no solo con Estados Unidos sino con Naciones Unidas. El objetivo principal de esta estrategia es garantizar la coherencia y las capacidades para proteger el ciberespacio.

Y como objetivos estratégicos puede fortalecer la seguridad informática en cuanto la administración pública la cual mejorara aún más con la protección de sus sistemas esto se implementaría en crear una común infraestructura de red uniforme y segura como base de esta se tendría en cuenta la comunicación electrónica de audio y datos.

En este objetivo también se resaltarían los intereses del sector privado para protegerse contra el crimen y el espionaje en el ciberespacio cada sector tanto como el público y el privado debe tomar las medidas necesarias en el ámbito de la seguridad cibernética, cada sector debería evaluar y coordinar con las autoridades competentes y socios de la industria la seguridad informática.

Mejorar el control del ciberespacio, este tiene que reforzarse en la parte de protección contra el espionaje y el sabotaje, para eso Colombia puede intercambiará conocimientos en esta área, y también establecer el trabajo conjunto con las industrias, para esto necesitara la ayuda de organismos competentes encargados de hacer cumplir la ley que actuarían en forma de asesoramiento, y para hacer frente al crecimiento de los desafíos en las actividades mundiales de delitos cibernético se puede hacer un esfuerzo para lograr la cooperación global en el derecho penal basado en el delito cibernético del Consejo de Europa.

Otro objetivo estratégico seria la implementación de un sistema, que respalde firmemente la seguridad y que tenga en cuenta los aspectos tanto sociales y económicos, con eso se intensificaría la investigación sobre la seguridad en la información, además de esto se fortalecería el desarrollo tecnológico en Colombia.

Conclusiones

En los últimos años las tecnologías de la comunicación y de la información han tenido una gran evolución y se han implementado diferentes controles en cuanto al tema de la ciberseguridad en Colombia

Colombia ha tenido en estos últimos años un progreso en los temas de ciberseguridad y se han gestionado los temas de protección a la información en la red, y con esto la sensibilidad a los ciudadanos, por ello haciendo un análisis de todo lo expuesto en el trabajo se pueden sacar diferentes conclusiones frente al sistema nacional colombiano y el tema de ciberespacio, entre ellas se cuentan:

- Colombia tiene alta vulnerabilidad que frente al tema de ciberseguridad

- falta mayor participación en la cooperación internacional, para ejercer una administración más sólida.
- Ampliar el trabajo en la seguridad de la información tanto en el sector público como en el privado.
- Reforzar los temas de la ciberseguridad y la ciberdefensa con ayuda de entes internacionales.
- Sabiendo que la persona es el eslabón más débil, hay que trabajar fuertemente en campañas de concientización sobre la ciberseguridad y de cómo se puede prevenir.
- Tener capacidad de prevención de un delito de esta clase y de esta forma se puede disminuir la vulnerabilidad en las infraestructuras que puedan ser afectadas.
- el gobierno debe trabajar y mejorar en la creación de nuevas defensas e infraestructura a la hora de enfrentar un delito informático.
- Es también responsabilidad del Estado generar políticas de información hacia la población manteniéndolos consientes frente a la alta vulnerabilidad o amenaza cibernética.
- Es necesario hacer énfasis en la gestión de riesgos que tiene la ciberseguridad, especialmente con estrategias de prevención en el manejo de la información compartida, alertas, procesos seguros, etc..

Referencias Bibliográficas

López, D. (s.f). CONPES 3701: *Colombia hacia un futuro con ciberseguridad y ciberdefensa*. Universidad Piloto de Colombia. Bogotá. Recuperado 11octubre, 2018, de: http://polux.unipiloto.edu.co:8080/00002383.pdf

Departamento Nacional de Planeación. (2016). Documento CONPES 3854.Recuperado 5 de octubre, 2018, de: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Convenio sobre la ciberdelincuencia (2001) Recuperado de: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

III premio interamericano a la innovación para la gestión pública efectiva 2015. (2015, 23 agosto). Recuperado 8 octubre, 2018, de https://oas.org/es/sap/dgpe/innovacion/2015/docs/BasesPostulacions.pdf

Ley estatutaria No 1621. (2013, 13 abril). Recuperado 21 octubre, 2018, de BasesPostulacion_s.pdf

Molano, D. I. E. G. O. (2016, 11 abril). Vive digital [Ilustración]. Recuperado 1 noviembre, 2018, de https://www.mintic.gov.co

Caceres, J. A. I. R. O. Andres. (2016, 22 septiembre). Colombia en materia de ciberdefensa y ciberseguridad. Recuperado 6 noviembre, 2018, de https://dialogo-americas.com/es/articles/cyberdefense-and-cybersecurity-colomb