IMPORTANCIA DE LA CIBERSEGURIDAD EN COLOMBIA

Pérez Pérez Yuly
perezperezyuly@gmail.com
Universidad Piloto de Colombia

Resumen-La administración de la información económica y social en Colombia y el uso de tecnologías para esto, va en aumento y complejidad cada día, por esto mismo es preciso adquirir prácticas que mejoren y brinden soporte a los procesos de las entidades, teniendo en cuenta los riesgos inherentes de seguridad.

Lograr mantener la integridad, confidencialidad y disponibilidad en la información, es básico si se pretenden lograr los objetivos corporativos. Para que los anteriores principios sean efectivos, se requiere la implementación de pautas que sean adoptadas como cultura en las Entidades, lo cual implica un compromiso verdadero de todas las personas involucradas en su gestión.

Éste documento dará un enfoque para conocer algunos lineamientos de política de ciberseguridad en Colombia, legislación relacionada, antecedentes y conceptos propios de la ciberseguridad.

Abstract - The administration of the economic and social information in Colombia and the use of technologies for it, are increasing every day, so it is necessary to acquire practices that improve and support the processes of the entities, taking into account the risks of Security.

Maintain integrity, confidentiality, and availability of information is essential to achieving the corporate goals. For the above principles to be effective, it is necessary to implement guidelines that are adopted as a culture in the Entities, that implies a true commitment of all the people involved in its management.

This document will offer an approach to know some guidelines of cyber security policy in Colombia, related legislation, past and concepts specific to cybersecurity.

Palabras claves – Ciberataque, ciberdefensa, ciberespacio, ciberseguridad, confidencialidad, disponibilidad, integridad, seguridad de la información, seguridad digital, vulnerabilidades.

I. INTRODUCCIÓN

Actualmente, Colombia ha estado a la vanguardia en el campo de la seguridad de la información, donde se ha tomado la tarea de planear, implementar, evaluar y exigir el cumplimiento de políticas y/o procedimientos para la prevención de ataques cibernéticos y en consecuencia, proteger a los colombianos y su socio-economía de potenciales amenazas.

La delincuencia en el ciberespacio y sus secuelas cada día son más latentes y reales, dado que sus riesgos podrían causar tanto impacto, como otro tipo de delincuencia.

Por esto mismo, el gobierno nacional ha tomado la iniciativa para adoptar buenas prácticas y estar preparando ante la cantidad de formas empleadas por los ciberdelincuentes para atacar.

Con la expedición del documento Conpes 3854 del 11 de abril de 2016, el cual comprende de manera detallada la política pública en ciberseguridad de Colombia, se busca dar un punto de partida para la elaboración de estrategias de prevención y lucha contra los riesgos cibernéticos.

El Conpes de Seguridad Digital integra seis capítulos; introducción, antecedentes y justificación, marco conceptual, diagnostico, definición de la política y recomendaciones.

Conpes: El Consejo Nacional de Política Económica y Social, es la máxima autoridad nacional de planeación y se desempeña como organismo asesor del gobierno en todos los aspectos relacionados con el desarrollo económico y social del país. Para lograrlo, coordina y orienta

a los organismos encargados de la dirección económica y social en el gobierno, a través del estudio y aprobación de documentos sobre el desarrollo de políticas generales que son presentados en sesión.

El Departamento Nacional de Planeación desempeña las funciones de Secretaría Ejecutiva del Conpes, y por lo tanto es la entidad que coordina y presenta todos los documentos para discutir en sesión.

II. CIBERSEGURIDAD

A. Definición

Conjunto de respuestas que un Estado y/o entidad estima necesario adoptar para hacerle frente a conductas consideradas reprochables o causantes de perjuicio social, con el fin de garantizar la protección de los intereses esenciales de los mismos y de los derechos de los residentes en el territorio bajo su jurisdicción.

En otras palabras, su objetivo es gestionar los riesgos que vienen del ciberespacio, relacionados con la información digital y sus sistemas interconectados, donde el ciberespacio se relaciona con internet. (MicTc, 2014)

B. Elementos de la Ciberseguridad

Figura 1. Elementos fundamentales de la ciberseguridad

Fuente: Autor del artículo

Confidencialidad: propiedad de que la información no sea divulgada o accedida a personas, entidades o procesos no autorizados.

Disponibilidad: propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.

Integridad**:** propiedad de conservar la exactitud e integridad de los activos de información.

Riesgo de seguridad digital: es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital.

Gestión de riesgos de seguridad digital**:** es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. (Conpes 3854, 2016)

Delito informático: es todo aquello acto ilegal o no autorizado que impide el procesamiento de datos en un sistema informático.

El ciberdelito: forma del delito informático que emplea tecnologías de internet para su desarrollo, es decir, delitos realizados en el ciberespacio.

C. Objetivo

Implementar instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional. (Conpes 3701, 2011)

III. CARACTERÍSTICAS DE LOS CIBERATAQUES

Hoy en día la tecnología nos presta infinidad de maneras para explotar las vulnerabilidades, entre ellas están el internet, herramienta con la que podemos lograr lo siguiente:

A. Apropiación de credenciales

Algunas de las principales formas para la obtención de credenciales de conexión a los sistemas son:

- Obtención directa: el usuario entrega directamente sus datos al atacante.
- Obtención por engaño al usuario: el atacante se hace pasar por administrador y solicita credenciales al usuario con motivo de soporte técnico.
- Obtención por escucha de tráfico: el atacante intercepta los datos trasmitidos por medios no seguros, sin cifrado o monitoreo de tráfico.

- Obtención por medio de aplicaciones: uso de virus en los equipos de los usuarios, guardan sus parámetros de conexión a sistemas.
- Obtención por acceso a archivos de credenciales.
- Obtención por descifrado de credenciales cifradas.
- Obtención por observación a los usuarios.

Una vez se tengan las credenciales de acceso, resulta muy fácil penetrar en los sistemas de manera no autorizada y alterar la integridad y disponibilidad de los mismos.

B. Ataques de denegación de servicios

Quizás el más usado, donde se abusa de los recursos disponibles de los usuarios, se trata de sobrecargar con solicitudes los sistemas informáticos, denegando su acceso y disponibilidad, algunas de sus representaciones son buffer overflow e inundación de mensajes.

C. Ataque por cambio de la página web

Este ataque se relaciona con el término defacement, donde el contenido de la página es alterado. Una variedad de este tipo de ataques es cuando se redirige al usuario a un sitio falto, pero es copia exacta del sitio deseado, se realiza con el fin de obtener datos como los de las tarjetas de crédito, de aquí la palabra phishing.

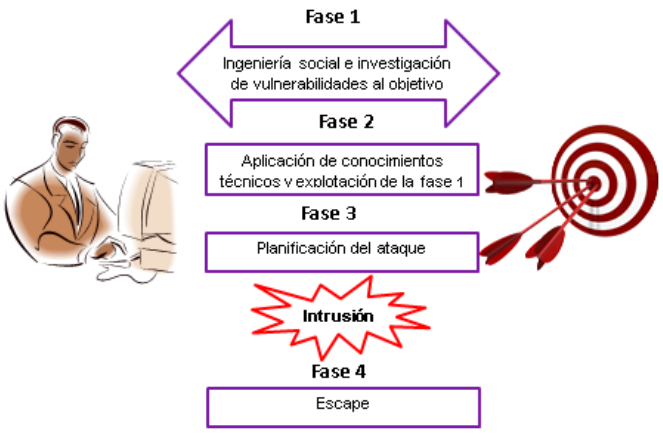
D. Alteración de protocolos de comunicación

El conocer la operación de los diferentes protocolos (Tcp/Ip, Udp, Icmp) y sus limitaciones, permite paralizar la red, reencaminar paquetes Ip hacia destinos falsos, aumentar la carga de los sistemas, impedir la comunicación entre emisor y receptor, entre otros.

E. Modelo de ciberataque

Un modelo de desarrollo de un ciberataque, básicamente comprende cuatro fases. La fase 1, comprende la investigación y obtención de información, la técnica más usada es ingeniería social, aquí se conocen los mecanismos empleados por los usuarios como autenticación y su nivel de seguridad. En la fase 2 y 3, por medio de conocimientos técnicos del atacante, herramientas disponibles y uso de los elementos de la fase 1 se realiza la intrusión a los sistemas. En la fase 4, su objetivo es evitar que sea detectado el origen del ataque, por eso es común el uso de alias o el uso de identidades digitales falsas, incluso el borrado de rastros que impidan la llegada al atacante.

Figura 2. Fases del ciberataque



Fuente: Seguridad de TI y Telecomunicaciones. Solange Ghernaouti

IV. NORMATIVIDAD APLICABLE A LA CIBERSEGURIDAD EN COLOMBIA

A. Constitución Política de Colombia

Principalmente, la Constitución Política de Colombia en su artículo 15 dice: 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 los bancos de datos y en archivos de entidades públicas y privadas.

Artículo 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.

Artículo 29. El debido proceso se aplicará a toda clase de actuaciones judiciales y administrativas.

Nadie podrá ser juzgado sino conforme a leyes preexistentes al acto que se le imputa, ante juez o tribunal competente y con observancia de la plenitud de las formas propias de cada juicio. En materia penal, la ley permisiva o favorable, aun cuando sea posterior, se aplicará de preferencia a la restrictiva o desfavorable. Toda persona se presume inocente mientras no se la haya declarado judicialmente culpable. Quien sea sindicado tiene derecho a la defensa y a la asistencia de un abogado escogido por él, o de oficio, durante la investigación y el juzgamiento; a un debido proceso público sin dilaciones injustificadas; a presentar pruebas y a controvertir las que se alleguen en su contra; a impugnar la sentencia condenatoria, y a no ser juzgado dos veces por el mismo hecho. Es nula, de pleno derecho, la prueba obtenida con violación del debido proceso.

B. Ley 527 de 1999

Ley del comercio electrónico, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

C. Ley 594 de 2000

Por medio de la cual se dicta la Ley general de archivos y establece reglas y principios generales que regulan la función archivística del Estado.

D. Ley 599 de 2000

Por la cual se expide el código penal colombiano.

E. Ley 600 de 2000

Por la cual se expide el Código de Procedimiento Penal.

F.Ley 679 de 2001

Esta ley tiene por objeto dictar medidas de protección contra la explotación, la pornografía, el turismo sexual y demás formas de abuso sexual con menores de edad, mediante el establecimiento de normas de carácter preventivo y sancionatorio.

G. *Ley 906 de 2004*

Por la cual se expide el código de procedimiento penal (corregida de conformidad con el Decreto 2770).

H. Ley 962 de 2005

Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de ló el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados.

I. Ley 1032 de 2006

Por la cual se modifican algunos artículos del código penal, sobre la violación a los derechos patrimoniales de autor y derechos conexos.

J. Ley 1273 de 2009

Esta ley creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión y multas.

V. ANTECEDENTES EN COLOMBIA

Aunque los medios de comunicación visuales en Colombia no dedican tanto espacio a las noticias de ciberataques, si lo están haciendo las revistas y periódicos nacionales como: Semana, El Tiempo, El Heraldo, entre otros, los cuales muestran que es un hecho real que el país si sufre ciberataques diariamente de forma pasiva y activa, ya sea en las entidades financieras, del gobierno, privadas, universidades y ciudadanos. Esto ha generado impactos de millones de pesos porque en su mayoría no cuentan con planes de prevención y respuesta a esta clase de incidentes.

Algunos casos sonados a nivel nacional son:
En el año 2011, el conocido grupo Anonymous atacó los sitios web del Ministerio de educación, Senado, Ministerio de Defensa, Presidencia de la República y el sitio de Juan Manuel Santos.

En el año 2012, nuevamente este grupo se atribuye el ataque al sitio web de la policía.

Este año 2016, días antes del plebiscito, página de la Registraduría Nacional del Estado Civil sufre ataque.

El periódico El Tiempo, el 13 Julio de 2016, publico que en América Latina, Colombia es después de Brasil y México el tercer país con más ataques cibernéticos.

La página web del Centro Cibernético de la Policía Nacional de Colombia - CCPN, ofrece una plataforma llena de servicios, informes, boletines, reportes de incidentes y guías sobre la temática tratada, algunos casos conocidos aquí son:

- En la ciudad de Barranquilla, captura de organización dedicada a realizar defraudaciones millonarias a través de medios informáticos a diferentes entidades financieras. El posible hurto mediante la utilización de medios informáticos, un monto superior a los diez mil millones de pesos ($10.000.000.000), resultando afectadas 326 cuentas de esa entidad financiera, hechos relacionados con pagos de planillas de seguridad social a través de PSE. La modalidad delictiva empleada fue malware.

- En Bogotá capturan a alias 'Ellmo', sindicado por los delitos de demanda de explotación sexual comercial de persona menor de 18 años de edad y pornografía infantil a través de redes sociales.

- Captura de presunto experto informático, responsable de una millonaria defraudación ($541,412,000) a una reconocida aerolínea a través del hurto al sistema de acumulación de millas de la página life miles y hurtaba los datos personales de los diferentes viajeros mediante la utilización de programas como phishing, vishing y de ingeniería social.

Lo anterior, es una validación de la Figura 4, en la cual se muestra que el sector más afectado por los ciberdelitos son los ciudadanos.

Adicionalmente, según reporte de ciberincidentes extraído del Centro Cibernético de la Policía Nacional se puede observar las cifras en cuanto a modalidad y sector atacado para los meses de octubre y noviembre de este año, la mayoría de estos ataques son realizados en el centro del país:

Figura 3. Reporte por modalidad

Fuente: CCPN

Figura 4. Reporte por sector

Fuente: CCPN

VI. POLÍTICA NACIONAL DE CIBERSEGURIDAD

Colombia consiente de las necesidades y los problemas relacionados con la ciberseguridad, se comprometió una vez más con este tema, y ha gestionado la seguridad en el país en ambientes digitales.

El Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa y el Departamento de Planeación Nacional presentaron en abril de este año, el documento Conpes 3854, que describe la Política Nacional de Seguridad Digital. Este documento substituye al documento Conpes 3701 de 2011, el cual buscaba generar lineamientos de política de ciberseguridad y ciberdefensa enfocado a implementar una estrategia nacional que luchara contra el incremento continuo de las amenazas en el entorno informático, las cuales afectaban al país de manera significativa. Esta política se estableció hasta el año 2015, donde además se planteaba un frente de respuesta a las situaciones de riesgo de seguridad informática, para esta época la situación estaba bajo el cargo del Ejército y la Policía, pero con el documento actual se obliga a todas las entidades del Estado y demás involucrados a emprender la prevención y la mitigación de los riesgos informáticos.

A. Documento Conpes 3854, 11 Abril de 2016

Este documento establece la Política Nacional de Seguridad Digital, donde en primer lugar establece un marco institucional alrededor de la seguridad digital en el gobierno, brinda conceptos básicos, modela un esquema de gestión sistemática para los riesgos de seguridad digital, además, muestra los principios fundamentales por los que se rige la política, tales como salvaguardar los derechos humanos y valores fundamentales, adopta un enfoque incluyente y colaborativo que involucra a todas las partes interesadas, asegurar una responsabilidad compartida entre las partes interesadas y adopta un enfoque basado en la gestión de riesgos. En segundo lugar, relaciona unos antecedentes de la temática, diagnosticando el estado de la ciberseguridad en el país. En tercer lugar, define la política teniendo en cuenta la gestión de riesgos, partes interesadas, fortalecimiento de la defensa generando mecanismos continuos para promover la contribución en seguridad digital a nivel nacional e internacional, adicionalmente, valora el impacto económico de la política.

En este documento, se puede evidenciar un aumento de las habilidades y conocimientos técnicos de ciberdefensa y formas para proteger la infraestructura crítica del país que podría verse afectada gravemente su operación. Parte de las estrategias presentadas en este documento, proponen la creación de acciones para que los ciudadanos tomen conciencia sobre los riesgos informáticos y el cómo prevenirlos, así como la creación de instituciones que complementen la misión de los grupos de respuesta a emergencias cibernéticas.

B. Grupo de Respuesta a Emergencias Cibernéticas (Colcert)

Su responsabilidad central es la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual estará enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal será la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional.

Los objetivos principales de Colcert son:

- Coordinar y asesorar a entidades públicas, privadas y sociedad civil para responder ante incidentes informáticos.
- Presta servicios de prevención ante amenazas informáticas, respuesta a incidentes informáticos, sensibilización y formación en seguridad informática.
- Es el contacto internacional con organismos internacionales y sus homólogos en otros países.
- Promueve la creación de otras entidades que gestionen la operación frente a incidentes de ciberseguridad en las infraestructuras críticas nacionales, el sector privado y la sociedad civil.
- Desarrolla y promueve procedimientos, protocolos y guías de buenas prácticas y recomendaciones de ciberdefensa y ciberseguridad y vela por su implementación y cumplimiento.
- Coordina la ejecución de políticas e iniciativas público-privadas de sensibilización y formación de talento humano especializado, relativas a la ciberdefensa y ciberseguridad.

- Apoya al Estado en la prevención e investigación de delitos donde medien las tecnologías de la información y las comunicaciones.
- Y por último fomenta un sistema de gestión de conocimiento relativo a la ciberdefensa y ciberseguridad, orientado a la mejora de los servicios prestados por el Colcert.

C. CSIRT- CCIT

Es un centro de coordinación de atención a incidentes de seguridad informática en el país, el cual mantiene contacto directo con los centros de seguridad de las empresas afiliadas y cuenta con la capacidad de coordinar el tratamiento y solución de las solicitudes y denuncias sobre problemas de seguridad informática que sean recibidas en la cuenta de correo electrónico.

Este Centro también actúa como contacto nacional e internacional para la gestión y atención a incidentes de seguridad informática que involucren redes y/o servicios Colombianos.

VII. ¿QUÉ SE PUEDE HACER?

A. Contribuir al cumplimiento de los objetivos de ciberdefensa

Se contribuye al cumplimiento de los objetivos, replanteando la relación con las nuevas tecnologías y los proveedores, en el que se exija garantías de seguridad en la infraestructura y aplicaciones, plantear estrategias preventivas que protejan y defiendan los recursos sensibles y críticos de las organizaciones, el uso de productos de calidad en el que su nivel de seguridad puedas ser claro, transparente, controlable y verificable.

B. Generar conocimiento, capacitación y sensibilización

No es desconocido que en la actualidad se ha presentado un auge en la oferta de formación en temas de seguridad informática por instituciones educativas en Colombia, donde desde el pregrado han formado en aspectos de seguridad y a nivel de postgrado en especializaciones y maestrías.

Las entidades privadas y públicas preocupadas por todo lo que implica la seguridad han contribuido a patrocinar la educación de sus empleados y la implementación de buenas prácticas como los sistemas de gestión de seguridad informática, donde además de cumplir con un requisito legal son conscientes de la necesidad de implementar medidas que minimicen los riesgos informáticos.

La Escuela Superior de Guerra de Colombia ya ha realizado el lanzamiento de la maestría en Ciberseguridad y Ciberdefensa que permite que los servidores públicos adquieran los conocimientos, competencias y habilidades necesarias para prevenir y gestionar los riesgos de Seguridad Digital.

C. *Implementar planes de continuidad del negocio*

Una de las principales preocupaciones del Ministerio de Defensa es si sus líneas tecnológicas están preparadas para continuar con la operación en caso de un evento desastroso. Por esto, sus unidades militares de soporte tecnológico se encuentran implementando sistemas de gestión de seguridad informática donde le han dado gran importancia a la operación de planes de continuidad del negocio en sus tareas de desarrollo de inteligencia, en el que han establecido como su principal riesgo de continuidad el ciberataque, por esto, han invertido recursos tecnológicos, humanos y de conocimiento para la preparación ante este incidente.

No solamente las instituciones militares se encuentran en este proyecto sino grandes compañías ya lo han implementado o se encuentran en su construcción.

D. Respeto por la normatividad de seguridad

En el capítulo IV de este artículo, se muestran las principales normas que regulan la ciberseguridad y el desconocerlas no exime la responsabilidad en su incumplimiento.

E. Reducción de vulnerabilidades tecnológicas

La investigación de nuevas modalidades de delitos y ataques a través de internet permite conocer a fondo las vulnerabilidades, amenazas y

riesgos para así adoptar medidas y reducir su impacto.

Seguir estándares de buenas prácticas propuestos por organismos de reconocimiento internacional, favorece la reducción de debilidades tecnológicas.

F. *Establecer roles y responsabilidades en seguridad de la información*

Aquí es el debate sobre el área de las entidades a la cual debe pertenecer seguridad de la información, ¿de la Oficina de Tecnología?, ¿de la Dirección?, ¿de Control Interno? ¿De Planeación? ¿De la Administración General?.

En la mayoría de los casos, se ha evidenciado que un gran porcentaje de Compañías afirman que el área de Seguridad de la Información en sus empresas depende de la gerencia de TI. Sin embargo los estándares y las mejores prácticas propuestas por Organismos internacionales y profesionales en el tema, indican que el área de seguridad debe ser independiente de TI, lo cual genera más objetividad e imparcialidad, en cuanto a recursos y demás.

Ahora, para las Entidades que no cuenta con un área de seguridad conformada, ni con roles y responsables para la Seguridad de la Información establecidos e implementados, es tiempo de iniciar una protección adecuada de la información, para disminuir la probabilidad de la ocurrencia de incidentes.

VIII. CONCLUSIONES

Es indispensable establecer pautas que brinden altos niveles de seguridad en el entorno digital, como la implementación de políticas efectivas y velar por su cumplimiento.

Es necesario identificar los recursos implicados en la ciberseguridad y la clasificación de los mismos, para determinar su grado de criticidad y exposición. Cada recurso es objetivo de seguridad y por lo tanto requiere una adecuada gestión de sus riesgos, los mecanismos de seguridad inherentes y aplicables, así como las restricciones técnicas, en otras palabras controles.

Es claro que el eslabón más débil son las personas, por lo tanto requiere un trabajo intenso y constante donde a través de formación y concientización se inyecte la importancia de la ciberseguridad y su impacto.

El gobierno Colombiano brinda herramientas y conocimiento sobre la ciberseguridad disponibles a los ciudadanos, de tal manera que solo queda entenderlas y hacer uso adecuado de ellas.

A nivel estratégico, es fundamental garantizar la comunicación de estrategias de prevención, información compartida, procedimientos y gestión de alertas. Además, es necesario dar a conocer las prácticas óptimas para la gestión del riesgo y de la seguridad.

Colombia ha contribuido al cumplimiento transparente, controlable y verificable de normas de seguridad, reducción de vulnerabilidades de la tecnología y las soluciones de seguridad.

De la ciberseguridad no se obtienen beneficios económicos, por el contrario es una inversión costosa y constante pero si aporta a la reducción de pérdidas e impactos.

En Colombia la propensión en términos generales es que las pymes y grandes empresas, no se han apropiado de una cultura de prevención y por lo tanto los recursos asignados para generación de controles internos y externos con el fin de mitigar los riesgos de ataque no se han incrementado, es decir son limitados, cuando si los ciberataques tienden a crecer y donde nuevas amenazas como el ramsomware, botnets, malware, phising, defacement, secuestro de información, DOS, ataques de ingeniería social, entre otros, se constituyen en los retos primordiales a enfrentar en un plazo inmediato.

REFERENCIAS

[1] http://www.colcert.gov.co/

[2] http://www.csirt-ccit.org.co/

[3] http://www.ccp.gov.co/

[4] Conpes 3701, D. N. (2011). *Conpes 3701*. Bogotá: Consejo Nacional de Política Económica y Social.

[5] Conpes 3854, C. N. (4 de Octubre de 2016). *Departamento Nacional de Planeación*.

[6] Giant, N. (2016). *Ciberseguridad para la i-generación.* Madrid: Narcea, S.A. De Ediciones.

[7] MicTc, M. d. (2014). *Agenda Estratégica de Innovación: Ciberseguridad.* Bogotá.

[8] Moreno, J. Z. (2015). *Ciberdiccionario.*

[9] Telefónica, F. (s.f.). *Ciberseguridad, la protección de la información en un mundo digital.* Ariel.

[10] *Guía de Ciberseguridad para los países en desarrollo*, Unión Internacional de Telecomunicaciones, 2007.

Autor

Yuly Pérez Pérez: Ingeniera de Sistemas de la Universidad Cooperativa de Colombia, Sede Bucaramanga, año 2014.
Estudiante de Especialización en Seguridad Informática de la Universidad Piloto de Colombia, Bogotá, año 2016.