DOCUMENTO CONPES 3701 LINEAMIENTOS DE POLÍTICAS PARA CIBERSEGURIDAD Y CIBERDEFENSA

Wilson Bernardo Guerrero Romero
willrom@hotmail.com
Seminario de Investigación Aplicada, Universidad Piloto de Colombia

Resumen: Breve análisis del documento CONPES 3701, en el cual se aborda una estrategia para afrontar las diferentes amenazas, a las que se encuentran significativamente expuestas las entidades del país, mediante la inclusión del tema "ciberdefensa y ciberseguridad" en el Plan Nacional de Desarrollo, que busca fortalecer las capacidades del Estado y mitigar el impacto de dichos ataques.

Además menciona las leyes y organismos con los cuales se debe apoyar la Nación, para realizar la gestión del manejo de respuesta a incidentes.

Índice de Términos: Ciberseguridad, ciberdefensa, ciberespacio, ciberdelito, CERT, CONPES, amenaza informática.

Abstract: A short analysis from the document CONPES 3701 is approached, where an strategy to face different threads to which Colombian entities are significantly exposed through the inclusion of the topic "cyber defense and cyber security" in the National Plan of Development searching for strengthening the capacities of the state to reduce the impact of such attacks.

Besides, it talks about the laws and organs that support the nation to carry out the management of incidents response.

Key Words: Cybersecurity, cyberdefence, cyberspace, cybercrime, cert, CONPES, computer threat.

I. INTRODUCCIÓN

Debido al gran crecimiento que ha tenido la tecnología a nivel mundial, y a las continuas noticias de ataques informáticos, ha hecho que tanto las empresas privadas como las del estado, deben estar a la vanguardia de los avances tecnológicos, para enfrentarse a los nuevos escenarios de riesgos y amenazas, por tal motivo mediante este articulo realizamos un análisis del documento CONPES (Consejo Nacional de Política Económica y Social) 3701 en el cual nos presenta un resumen donde muestra que, Colombia alcanzo hasta el 2010 un número de subscripciones de internet de 4.384.181, pero que según un último reporte de la página www.mintic.gov.co muestra que en el primer trimestre del 2015, se tienen un número de 10.724.350 suscripciones, lo cual nos da un crecimiento durante estos cuatro años y medio del 59.1%, de los cuales 5.3 millones corresponden a internet fijo y 5.4 millones a subscripciones móviles. De igual manera el Ministerio de Tecnologías de la Información y las telecomunicaciones (MINTIC), basado en las encuestas informa que el 80% por ciento de los colombianos utiliza internet [1].

Basados en el crecimiento del uso de las tecnologías que conlleva de manera relativa a un incremento en las amenazas y teniendo en cuenta los ataques cibernéticos a los que se vieron expuestos en varias ocasiones, además del crecimiento de las denuncias impuestas por los colombianos en los cuales se atentaba contra la ley 1273 de 2009, se ven obligados a realizar lineamientos de políticas y montajes de diferentes estrategias, donde nos daremos cuenta que una vez terminado el documento CONPES en julio 14 de 2011, uno de los pasos más importantes fue la implementación del CERT (Computer Emergency Response Team) también conocido como CSIRT (Computer Security and Incidente Response Team), ya que Colombia a la fecha de julio 14 de 2011 no estaba dentro de los 13 países de la región que contaban con dicho equipo, pero que a partir de la circular interna 0335 del 1 de septiembre de 2011 fue implementada, y se conoce como COLCERT.

Pero para entrar en contexto, primero daremos una breve explicación de ciberdefensa y ciberseguridad y luego entraremos en el significado del CONPES.

II. CIBERDEFENSA Y CIBERSEGURIDAD

La ciberdefensa y ciberseguridad nace de la necesidad de las organizaciones del Estado de proteger los sectores críticos de servicios como el suministro de agua, energía eléctrica, producción, almacenamiento y suministro de gas y petróleo, bancos y finanzas, telecomunicaciones, transporte servicios de emergencia y operaciones gubernamentales, de los diferentes ataques y responder a la continua evolución y el acceso masivo de equipos de comunicación como (computadores, tablets, celulares y demás dispositivos electrónicos) de amenazas, mediante estrategias que garanticen una continuidad del negocio y protección de la información, así se considera la ciberdefensa y la ciberseguridad como la capacidad de los estados para enfrentar los ataques que atentan contra la seguridad en el ambiente cibernético.

Pero la ciberseguridad también se conoce como la seguridad informática y esta nos lleva al objetivo de la protección de computadores, redes, programas y datos disponibilidad, integridad y confidencialidad [2]. La diferencia entre la ciberseguridad y ciberdefensa radica que la ciberdefensa se encarga de prevenir y contrarrestar las amenazas, y la ciberseguridad es la que minimiza el nivel de los riesgos, pero que en términos globales la una es el complemento de la otra para proteger la soberanía nacional.

III. CONSEJO NACIONAL DE PLANEACIÓN (CONPES)

El CONPES es una entidad encargada de presentarle al Gobierno Nacional, elementos como políticas, planes, programas, estrategias y proyectos encaminados al desarrollo económico y social del país. Esta organización fue creada en 1958 bajo la ley 19, la cual buscaba reorganizar el manejo de la administración pública, con el objetivo de mejorar la coordinación de los proyectos de desarrollo que se querían ejecutar [3].

Una vez establecido el CONPES, se decreta que el objetivo principal es el de coordinar y diseñar políticas para el manejo del presupuesto de los recursos de inversión, además de enlazar las entidades de planeación del Gobierno con los demás niveles del mismo. Con el decreto 1832 del 31 de agosto de 2012 establece que está dentro de las funciones el realizar seguimiento a los planes, proyectos y programas del sector público, además de realizar un seguimiento constante y permanente a la economía nacional e internacional, y por otro lado el de presentar y proponer nuevos programas y proyectos con el objetivo de mejorar en el desarrollo social, económico, ambiental e institucional, y de esta manera asesorar al Gobierno para establecer los mejores lineamientos en dichos procesos [4].

El CONPES es la máxima autoridad a nivel nacional para el desarrollo y la planeación, ya que esta debe coordinar y dirigir a los demás organismos, realizando la emisión de diferentes documentos, los cuales antes son debidamente analizados y aprobados junto con la presidencia de la Republica. Esta organización está integrada por el Presidente de la República, Vicepresidente de la República, Ministros de Interior, Justicia, Relaciones Exteriores, Hacienda, Defensa Nacional, Agricultura, Protección Social, Minas y Energía, Comercio, Industria y Turismo, Educación Nacional, Ambiente, Vivienda y Desarrollo Territorial, Comunicaciones, Transporte, Cultura, Director del Departamento Administrativo de la Presidencia de la República, Director del Departamento Administrativo de Ciencia y el Director del Departamento Nacional de Planeación [5].

IV. OBJETIVOS DEL DOCUMENTO CONPES (3701)

El objetivo principal del documento CONPES es el fortalecimiento de la capacidad del estado para enfrentar las amenazas que atentan contra su seguridad y defensa, basado en las tres problemáticas que se identificaron en el país:

1) Falta de coordinación en operaciones de ciberseguridad y ciberdefensa: se habla de una falta de concientización, transmisión y cultura en el manejo seguro de la información en sectores públicos, privados y sociedad civil.

2) Falta de personal capacitado en especialidades de ciberseguridad y ciberdefensa: en el momento de la presentación del documento, se evidencia un déficit en la educación de los temas descritos, por esta razón muchas de las personas interesadas se veían obligadas a obtener estos conocimientos a nivel extranjero, pero por ser un recurso más costoso, no tenía un acogimiento representativo y esto conllevaba a la perdida de casos por el mal manejo en procedimientos como la cadena de custodia.

3) Debilidad en la regulación y legislación de la protección de la información de los datos: se reflexiona a la legislación que se tenía en el momento y que a partir de esta debe ser modificada, basados en los lineamientos a nivel mundial como la de la convención del Consejo de Europa en delitos cibernéticos, que establece una cooperación judicial.

Para el cumplimiento del objetivo y afrontar las tres problemáticas planteadas se determina la necesidad de la implementación de los siguientes lineamientos:

1) Conformar tres instancias (COLCERT, CCP, CCOC) con las cuales no se contaban en la realización de dicho documento (CONPES 3701), a continuación un grafico referente a la implementación de dichas instancias [6].

Grafica No. 1 Modelo de Coordinación ministerio de defensa, 2011, Fuente Documento CONPES 3701 Ministerio de Defensa Nacional

Dentro de la investigación que se realizó, se evidencio el funcionamiento de las tres organizaciones. COLCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia 'http://www.colcert.gov.co'), pagina que cuenta con los siguientes sitios de interés como:

- Alertas de seguridad: donde encontraremos noticias de las alertas a vulnerabilidades de diferentes marcas tecnológicas como Apple, Microsoft, Oracle, IBM entre otros; y en algunos casos incluyen el código CVE correspondiente a la vulnerabilidad con respecto a ciberdefensa y ciberseguridad.
- Eventos de ciberseguridad: diferentes actividades de concientización, mediante conferencias y seminarios que tendrán lugar en el futuro o que se llevaron a cabo en el pasado.
- Contáctenos: es un espacio donde fomentan una retroalimentación en base a comentarios y sugerencias de la pagina, e inclusive el de interactuar con los usuarios para recibir tips de seguridad.
- Denunciar ciberdelitos: breve descripción de la manera como debemos realizar una denuncia de ciberdelitos, ya que estamos obligados hacerlo mediante el artículo 67 de la ley 906 de 2004.
- Reportar incidente: formulario para realizar los diferentes reportes de incidentes que servirán para que el gobierno pueda determinar el nivel de aceptación de los mismos.
- Acerca de: misión y objetivos del COLCERT.
- Recursos: diferentes talleres en pro de presentar a la comunidad lecciones aprendidas frente al tema.

A continuación se resumen los objetivos del grupo de respuesta a emergencias cibernéticas (COLCERT):

- Coordinar, asesorar y crear los CSIRT's a nivel nacional, para realizar el apoyo a entidades del nivel público, privado y de la sociedad civil para el buen manejo ante incidentes informáticos.
- Ofrecer y recomendar, servicios de prevención, respuesta a incidentes y contacto directo con homólogos en otros países, así como con organismos

internacionales para mejorar el manejo de amenazas informáticas.

- Coordinar, desarrollar, promover y ejecutar procedimientos, políticas que contribuya en el manejo de sensibilización y buenas prácticas, encaminadas a realizar recomendaciones de ciberdefensa y ciberseguridad para las infraestructuras críticas.
- Promover un sistema de gestión de conocimiento frente a la ciberdefensa y ciberseguridad, en mejora de minimizar las diferentes amenazas.

Como se detalló anteriormente el COLCERT está encargado de coordinar todo lo referente a los aspectos de ciberseguridad y ciberdefensa, por tal motivo le prestara apoyo a las demás áreas como lo son el CCP (Centro Cibernético Policial), encargado de proteger, responder y divulgar a la ciudadanía todo lo relacionado con amenazas y delitos cibernéticos, orientado a resguardar la disponibilidad, integridad y confidencialidad de la información, que estará en cabeza de la Policía Nacional, y el CCOC (Comando Conjunto Cibernético), encargado de fortalecer, monitorear y desarrollar capacidades tanto técnicas como de infraestructura, que permitan afrontar las amenazas y ataques cibernéticos que atenten contra la seguridad y defensa nacional, y que estará en cabeza del comando general de las Fuerzas Militares [7], [8].

2) Capacitación especializada a funcionarios que estén relacionados actualmente con la ciberseguridad y ciberdefensa y básicamente con el manejo y atención a incidentes de seguridad. El COLCERT cuenta con el apoyo del Comité Internacional Contra el Terrorismo (CICTE).

En la actualidad a parte de la gran cantidad de esfuerzos de la Nación, también están un sin número de entidades que se preocupan por las mismas problemáticas y de esta manera universidades y organizaciones prestan el servicio de capacitación y socialización de los mismos temas, tales como la Cámara Colombiana de Informática y Telecomunicaciones, quien a la fecha ha realizado dos foros en el tema de ciberseguridad y ciberdefensa, donde la temática estaba basada en las tendencias, retos y oportunidades planteadas por los diferentes organismos, encaminadas a mitigar o contrarrestar los efectos de los delitos cibernéticos en Colombia [9].

3) Para la solución de la tercera problemática se encaminaron esfuerzos en la búsqueda de herramientas judiciales para la efectiva prevención, investigación y judicialización de los delitos cibernéticos, para lo cual el documento hace referencia al siguiente marco legal.

- Ley 527 de 1999 comercio electrónico: donde se reglamenta el uso y acceso de mensajes de datos, comercio electrónico y firmas digitales, además de establecer cuáles son aquellas organizaciones que pueden certificar dichos procesos.
- Ley 599 de 2000: en el capítulo VII, articulo 192 violación ilícita de comunicaciones, menciona que el que ilícitamente substraiga, oculte, extravié, destruya, intercepte, controle o impida una comunicación privada dirigida hacia otras personas o entidades, serán privados de la libertad y si además se revela el contenidos, o lo emplea en provecho propio este tiempo se duplicara.
- Ley 962 de 2005 denominada ley anti tramites: esta ley se caracteriza por incentivar el uso de la tecnología para aquellas organizaciones del estado o similares que realizan procedimientos de servicios públicos.
- Ley 1150 de 2007: en esta ley se establece que para la contratación con los recursos públicos se deben realizar mediante el sistema electrónico de contratación pública (SECOP).
- Ley 1273 de 2009: quizás la más importante hasta el momento en cuanto a sistemas informáticos se refiere, ya que con esta se modifica el código penal por el concepto de ley de la protección de la información y de los datos. En los cuales se tipifican los siguientes casos; acceso abusivo a un sistema informático, obstaculización ilegitima de sistema informático o red de telecomunicación, interceptación de datos

informáticos, daño informático, uso de software malicioso, violación de datos personales y suplantación de sitios web para capturar datos personales [10].

- Ley 1341 de 2009: se definen conceptos y principios sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones (TIC)
- Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009: establece la obligación para los proveedores de redes y/o servicios de telecomunicaciones que ofrezcan acceso a Internet, de implementar modelos de seguridad que cumplan con los principios de confidencialidad, integridad y disponibilidad de los datos y elementos de red, así como medidas para autenticación y no repudio. Además esta resolución agrega al artículo 1.8 de la resolución CRT 1740 de 2007 las definiciones de autenticación, autorización, ciberespacio, ciberseguridad, confidencialidad de datos, disponibilidad, entidad, infraestructura critica, integridad de datos, interceptación, interferencia, interrupción, no repudio, pharming, phishing, software malicioso y vulnerabilidad [11].
- Circular 052 de 2007 (Superintendencia Financiera de Colombia): establece los estándares mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios [12].

Cabe mencionar la ley estatutaria 1581 de 2012 que hace referencia a la protección de datos personales, ya que aunque el documento no la relaciono por motivo de ser una ley que se expidió después del mismo, pero que sin embargo hace referencia al buen manejo que se le debe dar a la información de los usuarios en la red [13].

V. ANTECEDENTES

No podemos pasar por alto el tema de los antecedentes, ya que es una de las circunstancias por las cuales obliga a las diferentes organizaciones y estados, a tomar lineamientos y estrategias para poder mitigar dichos ataques. En esta sección tomaremos como referencia los mencionados en el documento CONPES, pero también relacionaremos unos en los cuales fueron determinantes para los diferentes cambios en la tecnología.

El primer ataque que se toma como referencias es lo sucedido en abril de 2007 en Estonia, donde se menciona que empezó días después de que el Gobierno decidiera trasladar un monumento de los militares caídos. Estos ataques fueron dirigidos a varias instituciones públicas, bancos, partidos políticos y medios de comunicación, en consecuencia el Gobierno de Estonia se vio obligado a cortar la línea de internet por varios días y formatear los equipos afectados, por otro lado tomaron la decisión en 2008 de implementar el Centro de Excelencia para la Cooperación en Ciberdefensa (CCD) en apoyo con la Organización del Tratado de Atlántico Norte (OTAN) [14].

El siguiente ataque representativo fue el 4 de julio de 2009 cuando una serie intrusiones cibernéticas afecto a más de 20 sitios web de Organismos Gubernamentales de Estados Unidos y Corea del Sur, incluida la Casa Blanca, estos ataques consistieron en poner demasiado lenta la red hasta interrumpir el acceso a la misma [15].

En marzo de 2010 la BotNet Mariposa, utilizando 13 millones de direcciones ip, en por lo menos 190 países alrededor del mundo, con el objetivo de obtener datos personales y financieros; Donde Colombia ocupo el 5 puesto con el 4.94% de la cantidad de equipos infectados.

Dentro del documento no se menciona el virus gusano Stuxnet, pero que sin duda marco un episodio bastante difícil en la industria mundial, ya que en julio de 2010 este virus capaz de internarse y tomar control de la maquinaria de las diferentes plantas como eléctrica, presas de agua, nucleares y otros complejos industriales, aunque no se registró ningún atentado, este malware podría ser utilizada para generar daños físicos. El país más afectado fue Irán [16].

Otro de los malware fue Duqu donde su primera detección fue el 1 de septiembre de 2011, y fue considerado por muchos como la evolución del Stuxnet, ya que fue creado por los mismos autores,

a diferencia de Stuxnet, el propósito de Duqu era recopilar datos y activos de información con el objetivo de realizar un ataque en el futuro más profundo y no solo a industrias nucleares si no a las demás industrias, Duqu básicamente es un troyano para obtener acceso remoto y esta no tiene la capacidad de auto-replicarse [17].

En mayo de 2012 aparece FLAME, donde muchos lo califican como más sofisticado que Duqu, ya que este es un conjunto de herramientas como backdoors, troyanos y gusanos, lo que le facilitaba la propagación por las redes o dispositivos extraíbles. Su objetivo era realizar ataques de ciber espionaje dirigidos en principio al oriente medio, con la utilidad de grabar audio, capturas de pantalla, pulsaciones de teclado, y captura de tráfico de red [18].

Posteriormente aparece Gauss en junio de 2012, fue descubierto por los conocimientos adquiridos de los ataques que se realizaron con el malware FLAME, también considerado como troyano para ciber espionaje, ya que su objetivo era conseguir información sensible, como credenciales de acceso y contraseñas bancarias de Oriente Medio [19].

Por último el conocido Octubre Rojo, el cual fue investigado por KASPERSKY en octubre de 2012 por sugerencia de sus clientes, este malware se encargaba de recolectar información de los sistemas utilizados y posteriormente desplegar módulos para capturar todo tipo de datos, el objetivo de este malware era recopilar información de instituciones gubernamentales, embajadas, investigación, nucleares, energéticas, petroleras y agencias aeroespaciales, y los países más afectados fueron Europa del Este, Unión Soviética, Asia Central, Europa Occidental y América del Norte, y se habla que este malware venia afectando desde 2007 [20].

VI. CERT O CSIRT

Con el objetivo de proteger la red de amenazas, fue creado en 1988 el Equipo de Respuestas ante Emergencias Informáticas (CERT) o sus siglas en inglés (Computer Emergency Response Team) o también llamado CSIRT (Computer security Incident Response Team), en consecuencia a que la red fuera infectada por un virus de tipo gusano, que invadía el 10% de la misma [21].

En el nivel mundial se encuentra el CERT en www.cert.org que se encarga de mejorar la seguridad y resistencia de los sistemas y redes informáticas, quienes hacen parte o son una división del SEI (Software Engineering Institute - Universidad Carnegie Mellon), este SEI quien realiza la actividad de ayudar a las organizaciones gubernamentales y de la industria en Estados Unidos a adquirir, desarrollar, operar y mantener un software de funcionamiento asegurado, además de libre de vulnerabilidades. Soportado por la universidad en los programas de ciencias de la computación y la ingeniería [22].

La división CERT trabaja en estrecha colaboración con el Departamento de Seguridad Nacional de los Estados Unidos en temas como seguridad en la red, gestión de incidentes, amenas internas y aseguramiento de software entre otros, realizando constantemente capacitación y sensibilización con cursos e informes, además de la creación de desarrollos en soluciones prácticas y aplicables, basados en la recopilación de la información de conocimientos adquiridos, más el análisis de datos y su respectiva investigación.

De igual manera Estados Unidos cuenta con el USCERT (Grupo de Respuesta a Emergencias Cibernéticas de Estados Unidos), el Nombre ‘CERT’ es una marca registrada por la Universidad de Carnegie Mellon, pero en su página se encuentran todos los procedimientos y formularios a los cuales todos aquellos que quieran pertenecer a este grupo de CSIRT lo pueden tramitar, actualmente se encuentran 140 organizaciones adjuntas a esta certificación [23].

Pero a nivel mundial también se encuentra FIRST que es otra organización con el objetivo de respuesta a incidentes. En la cual también se adquiere una membrecía con el objetivo que los equipos de respuesta a incidentes puedan responder con mayor eficacia a los incidentes de seguridad. La organización suministra acceso a las mejores prácticas, herramientas y comunicación de confianza con los equipos miembros, actualmente cuenta con 326 equipos de respuesta en 73 países, dentro de los que se encuentra el COLCERT de Colombia, FIRST fue fundada en 1990, con motivo

del segundo virus gusano llamado 'Gusano Wank' y los diferentes problemas que se presentaron con respecto a conexión, comunicación, zona horaria entre los diferentes CERT registrados hasta ese momento [24].

Y por último la OEA (Organización de los Estados Americanos), fundada en 1948 y cuyos objetivos son la paz, justicia y fomentar solidaridad entre sus estados miembros, esta organización en pro de mejorar su comunicación empieza a crear programas de mejora y en el 2000, se forma el de seguridad cibernética con la misión de fortalecer la seguridad cibernética, en el momento este programa cuenta con la comunicación de 34 CERT o CSIRTs para la mejora de sus lineamientos y políticas al respecto [25].

VII. PLAN DE ACCIÓN

En el plan de acción nos encontramos con un cuadro completo de 22 numerales, de los cuales se busca relacionar las diferentes entidades como el Departamento Nacional de Planeación, Ministerio de Defensa Nacional, Ministerio de Tecnologías de la Información y las Comunicaciones, Comisión de Regulación de las Comunicaciones, Ministerio del Interior y Justicia, DAS, Fiscalía General de la Nación, que tendrán que integrarse para cumplir con las diferentes designaciones o lineamientos.

VIII. FINANCIAMIENTO

El documento nos muestra un presupuesto para la implementación de COLCERT, CCP (Centro Cibernético Policial), CCOC (Comando Conjunto Cibernético), que sería del 2011 de 1.428.444.328, 2012 de 5.400.000.000, 2013 de 5.000.000.000 y 2014 de 4.600.000.000

Donde el presupuesto del 2011 será financiado con recursos de funcionamiento y los demás años con inversiones de tres proyectos.

IX. RECOMENDACIONES

Encontramos 3 grandes puntos de recomendaciones importantes para el éxito de la implementación de los lineamientos de ciberseguridad y ciberdefensa.

1) Implementar la institucionalidad apropiada: se evidencian 11 pautas generales que buscan la integración de 4 de las diferentes entidades como Ministerio de Defensa Nacional, Ministerio de Tecnologías de la Información y la Comunicación, Comisión de la Regulación de las Comunicaciones y el Ministerio del Interior y las Comunicaciones, donde se le solicita a cada una de estas las diferentes actividades que deben desarrollar para el cumplimiento de los objetivos.

2) Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberseguridad y ciberdefensa: se encuentran 7 pautas que involucran a las 4 entidades como Ministerio de Defensa Nacional, Ministerio de Tecnologías de la Información y la Comunicación, Fiscalía General de la Nación y el Departamento Administrativo de Seguridad, donde la conclusión general es la solicitud a cada una de estas de llevar a cabo un diseño e implementación de planes de capacitación.

3) Fortalecer la legislación y cooperación internacional en materia de ciberseguridad y ciberdefensa: este posee 4 pautas para las entidades como Ministerio de Relaciones Exteriores, Ministerio de Defensa Nacional, Ministerio de Tecnologías de la Información y la Comunicación, Ministerio del Interior y Justicia, las cuales buscan la integración para considerar las diferentes leyes y reglamentos, y que estas puedan ser modificadas.

Un total de 22 recomendaciones estratégicas para el cumplimiento de los objetivos del documento CONPES.

Para destacar los pasos que se llevaron a cabo para el cumplimiento de los objetivos fueron:

- Implementar y mejorar la institucionalidad adecuada.
- Fomentar programas de capacitación especializada.
- Fortalecer la legislación y la cooperación internacional.

X. ACTUALIDAD

De acuerdo a una lista que presenta la organización UIT (Unión Internacional de

Telecomunicaciones), y que refleja en su página el MINTIC (Ministerio de de Tecnologías de la Información y las Comunicaciones), la cual refleja los países que mejor manejan el tema de ciberseguridad donde en enero 8 de 2015 Colombia ocupa el quinto lugar de los países de América, y compartiendo el noveno a nivel mundial con países como Francia, España, Egipto y Dinamarca. Éste reporte tomado de 104 países que participaron en una evaluación dentro de la cual se basaron en cinco aspectos como medidas legales, técnicas, organizacionales, generación de capacidades y cooperación y en los cuales las mejores calificaciones para Colombia fueron en las medidas legales, organizacional y capacidades, y que se debe mejorar en los aspectos técnicos y de cooperación nacional e internacional [26].

XI. CONCLUSIONES

Dentro del análisis de este documento, nos podemos encontrar con diferentes eventos de seguridad y amenazas que no dejan de evolucionar y que por esas razones a nivel global se deben tomar políticas y lineamientos, además de investigaciones que conlleven día a día a adquirir un conocimiento para difundirlo, y de esta manera tanto entidades del gobierno como las empresas privadas, tomen conciencia de los riesgos a los que nos vemos expuestos al utilizar las herramientas tecnológicas.

No obstante tener la claridad que el Gobierno tiene diferentes recursos como el CSIRT y leyes como la 1273 de 2009, a los cuales la ciudadanía puede acceder para estar en una continua evolución y defensa de los delitos y ataques cibernéticos, y no solo esperar a que una circunstancia de estas nos suceda y reaccionar, si no para tener una postura preventiva, ya que como es bien sabido los riesgos no solo se presentan a nivel externo si no también internos.

BIBLIOGRAFÍA

[1] Ministerio de Tecnologias de la Informacion y Las Comunicaciones, «MINTIC,» 30 06 2015. [En línea]. Available: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf. [Último acceso: 24 07 2015].

[2] UMUC , «University of Maryland University College,» 01 01 2015. [En línea]. Available: http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm. [Último acceso: 16 08 2015].

[3] Secretaria General de la alcaldia mayor , «Secretaria General de la alcaldia mayor,» Ley 19 de 1958, 18 11 1958. [En línea]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=8271. [Último acceso: 6 08 2015].

[4] Departamento Nacional de Planecion, «Decreto 1832 de agosto de 2012,» 31 08 2012. [En línea]. Available: https://colaboracion.dnp.gov.co/CDT/Normatividad/DECRETO%201832%20DEL%2031%20DE%20AGOSTO%20DE%202012%20(2).pdf. [Último acceso: 31 08 2015].

[5] Secretaria General de la alcaldia mayor, «Decreto 2148 de 2009,» Decreto 2148 de 2009, 08 06 2009. [En línea]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36401. [Último acceso: 07 08 2015].

[6] Consejo Nacional de Politicas Economica y social, «Documento Conpes 3701,» Bogota, 2011.

[7] colCert, «Grupo de Respuesta a Emergencias Ciberneticas de Colombia,» 08 07 2013. [En línea]. Available: http://www.colcert.gov.co/. [Último acceso: 7 8 2015].

[8] Ministerio de defensa, «Asobancaria,» Juanita Rodriguez, 01 10 2011. [En línea]. Available: http://www.asobancaria.com/portal/pls/portal/docs/1/4397395.PDF. [Último acceso: 07 08 2015].

[9] CCIT, «Camara Colombiana de Informatica y Telecomunicaciones,» 01 08 2015. [En línea]. Available: http://www.ccit.org.co. [Último acceso: 09 08 2015].

[10] Ministerio de Interior y de Justicia, *Ley 1273 de 2009*, Bogota, 2009.

[11] Comision de Regulacion de comunicaciones, *Resolucion 2258 de 2009*, Bogota, 2009.

[12] Consejo Nacional de Politica Economica y Social, *Conpes 3701*, Bogota, 2011.

[13] Secretaria General de la Alcaldia Mayor, *Ley 1582 de 2012*, Bogota, 2012.

[14] Te interesa . Es, «Te Intersa . es,» 19 04 2013. [En línea]. Available: http://www.teinteresa.es/mundo/ataques-ciberneticos-importantes-fecha_0_904110101.html. [Último acceso: 10 08 2015].

[15] Agencia AP, Reuters, «La Nacion .com,» 09 07 2009. [En línea]. Available: http://www.lanacion.com.ar/1148526-eeuu-alarma-por-un-ataque-cibernetico. [Último acceso: 10 08 2015].

[16] Despierta al Futuro, «Despierta al Futuro,» 26 09 2010. [En línea]. Available: http://despiertaalfuturo.blogspot.com/2010/09/stuxnet-el-arma-del-siglo-xxi-puede.html. [Último acceso: 10 08 2015].

[17] Symantec, «W.32 Duqu The precursor to the next Stuxnet,» Security response, California, 2011.

[18] Kaspersky, «The Flame: Questions and Answers,» Securelist, Moscow, 2012.

[19] Kaspersky, «Kaspersky Lab Discovers 'Gauss' – A New Complex Cyber-Threat Designed to Monitor Online Banking Accounts,» Kaspersky lab, Moscow, 2012.

[20] Kaspersky, «Kaspersky Lab identifica la operación "Octubre Rojo", una avanzada campaña de espionaje cibernético dirigida a instituciones diplomáticas y gubernamentales en todo el mundo,» Kaspersky Lab, moscow, 2013.

[21] Software Engineering Institute, «CERT,» 27 04 2015. [En línea]. Available: http://www.cert.org/csirts/. [Último acceso: 07 08 2015].

[22] Software Engineering Institute , «SEI,» Carnegie Mellon University, 05 08 2015. [En línea]. Available: http://www.sei.cmu.edu. [Último acceso: 08 08 2015].

[23] CERT, «CERT Computer Emergency Responce Team,» 24 07 2015. [En línea]. Available: http://www.cert.org. [Último acceso: 08 08 2015].

[24] FIRST , «FIRST Mejora de la seguridad en equipo,» 01 01 2015. [En línea]. Available: http://www.first.org. [Último acceso: 09 08 2015].

[25] OEA , «Organizacion de los Estados Americanos,» 01 01 2015. [En línea]. Available: https://www.sites.oas.org. [Último acceso: 09 08 2015].

[26] MINTIC, «Ministerio de Tecnologias de la Informacion y las Telecomunicaciones,» 08 01 2015. [En línea]. Available: http://www.mintic.gov.co/portal/604/w3-article-8148.html. [Último acceso: 17 08 2015].

[27] Deparatamento Nacional de Planeacion, «DNP Deparatamento Nacional de Planeacion,» 30 06 2015. [En línea]. Available: https://www.dnp.gov.co/CONPES/Paginas/conpes.aspx. [Último acceso: 24 07 2015].

[28] MWR, «Cyber Defence protects your most important business assets against attack,» MWR Infosecurity, London, 2014.

Autor

Wilson Bernardo Guerrero Romero
Ingeniero de Sistemas de la Universidad Santiago de Cali
Aspirante a Especialista en Seguridad Informática Universidad Piloto de Colombia.
Ingeniero de Sistemas y Coordinador de Tesorería de Tejidos Gaviota S.A.S