CIBERDEFENSA Y CIBERSEGURIDAD EN EL SECTOR DEFENSA DE COLOMBIA

Wilmar Cárdenas Moreno
Especialización de Seguridad Informática
e-mail: wilmarc2012@hotmail.com
Universidad Piloto de Colombia
Junio de 2015

RESUMEN

El presente artículo trata de los conceptos, aplicaciones y ventajas, en materia de ciberdefensa y Ciberseguridad así como los delitos cibernéticos más utilizados. Se hará referencia a algunos antecedentes nacionales e internacionales los cuales deben ser el punto de partida para estructurar una política orientada a desarrollar una Estrategia de defensa Nacional. Para ello se establece el objetivo central, los objetivos específicos, el alcance y se definen los lineamientos principales del plan de acción, teniendo en cuenta el incremento de las amenazas informáticas que afectan significativamente el país. Como resultado se obtendrán las recomendaciones principales a las instituciones que tienen responsabilidad directa.

PALABRAS CLAVE: Ciberespacio, Ciberdefensa, Ciberseguridad, Seguridad de la Información, Ciberataques

ABSTRACT

The present article treats of the concepts, applications and advantages, as for cyber defense and Cyber safety as well as the most used cybernetic crimes. It will refer to some national and international precedents which must be the point of item to structure a politics orientated to developing a Strategy of National defense. For it there are established the central aim, the specific aims, the scope and the principal limits of the action plan are defined, bearing in mind the increase of the IT threats that affect significantly the country. Since result the principal recommendations will be obtained to the institutions that have direct responsibility.

KEY WORDS: Cyberspace, Cyber defense, Cyber safety, Information Security, Cyber-attacks

1 INTRODUCCIÓN

Son pocas las personas que tienen conocimientos en temas relacionados con Ciberdefensa y Ciberseguridad y son menos las personas que tienen conciencia de las amenazas y peligros que a través del Ciberespacio afronta el país y por ende puede afectar no solo a las Fuerzas Armadas sino a sus habitantes.

La defensa y protección del Ciberespacio, se ha convertido en uno de los retos más importantes del estado, debido a la continua evolución, crecimiento y complejidad de los ataques cibernéticos. De ahí surge la necesidad de disponer de personal idóneo que se adapte a entornos de continuos avances tecnológicos que permitan proteger al Estado ante posibles nuevas amenazas.
Para abordar con éxito esta problemática, se debe avanzar significativamente en sensibilización y organización en Ciberdefensa y Ciberseguridad.

2 CARACTERÍSTICAS GENERALES

¿Qué es Ciberdefensa?

Es la capacidad del Estado para cumplir con las responsabilidades que le permitan prevenir y contrarrestar toda amenaza o ataque de naturaleza cibernética que afecte los valores e intereses nacionales. También se conoce como el conjunto de acciones de defensa activas pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición.
Se ha planteado iniciar el proceso de la Ciberdefensa por la Inteligencia Informática con el Ciberespacio como ambiente, para poder obtener los elementos descriptores, que conformen la identificación de los escenarios y a la vez parametrizables amenazas, para poder dimensionar los riesgos y así posibilitar el diseño de los instrumentos de defensa.

¿Qué es Ciberseguridad?

Es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno, lo que conlleva a la existencia de una situación de normalidad donde la población goce de niveles apropiados para utilizar los medios cibernéticos libres de cualquier amenaza o peligro.

El aumento de la capacidad delincuencial en el ciberespacio, así como la utilización de nuevas tecnologías para generar amenazas informáticas, constituyen una preocupación común a nivel mundial

dado que impacta de manera significativa la seguridad informática de las diferentes empresas en los ámbitos tanto público y privado, como al ciudadano mismo.
Si bien es cierto que la necesidad del Estado en aspectos de seguridad de la información es un factor crítico que requiere ser atendido, este es un campo muy amplio que abarca diferentes conceptos de seguridad física como de seguridad lógica (aplicación de barreras y procedimientos que resguarden la información), para proteger todos los medios en donde se encuentra la información. Sin embargo, el presente documento se enmarca en el contexto de Ciberseguridad y ciberdefensa, sin dejar de lado la posibilidad de que a futuro sea fortalecido por estrategias o mecanismos necesarios en seguridad de la información.

Debido a que el Gobierno Nacional requiere conocer y actuar de una forma integral frente al manejo de la información, es necesario contar con las instancias adecuadas que permitan ejercer una labor de "Ciberseguridad" y "ciberdefensa" frente a cualquier amenaza informática o ataque cibernético que pueda comprometer la información o afectar la infraestructura critica del país y poner en riesgo la seguridad y defensa del Estado.

En esta nueva era cibernética se hace necesario garantizar la seguridad de la información o por lo menos brindar pautas para que esta pueda ser segura dentro de determinados lineamientos, siendo cualquiera el carácter de la misma, sobre todo cuando es confidencial y puede afectar a una persona, a un grupo o a la Nación completa.

3 ANTECEDENTES

Como referentes de la normativa internacional en la materia es importante hacer mención de los siguientes esfuerzos:

La Organización de las Naciones Unidas – ONU ha abordado el tema desde 1998 bajo la denominación "Los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional", mediante la cual la Asamblea exhorta a los estados miembros a continuar promoviendo la revisión de los conceptos internacionales pertinentes encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones.

El Consejo de Europa adoptó en noviembre de 2001 el Convenio sobre Ciberdelincuencia (CCC, por sus siglas en inglés), entrado en vigor desde el 1° de julio de 2004, único instrumento vinculante vigente sobre el tema en el ámbito internacional, y su protocolo para la criminalización de actos de racismo y xenofobia cometidos a través de sistemas informáticos**.**

En el ámbito hemisférico, la Asamblea General de la Organización de los Estados Americanos adoptó mediante la Resolución AG/RES 2004 (XXXIV-O/04) la Estrategia Integral para combatir las amenazas a la seguridad cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de la seguridad cibernética.

La Comunidad Andina, en el ámbito regional, adoptó el 10 de julio de 2004 la Decisión 587, por la que 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.

En el ámbito Nacional en 2011, se produjo la promulgación de la Visión del JEMAD de la Ciberdefensa militar, en la que se definen las implicaciones en el uso del ciberespacio derivadas del concepto de la estrategia militar. En marzo de 2013 se firmó un convenio de colaboración entre el Instituto de Tecnologías de la Comunicación (INTECO), dependiente del Ministerio de Industria, y el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), del Ministerio del Interior, para actuar de forma coordinada ante ataques cibernéticos a este tipo de infraestructuras. Gracias a este acuerdo, se ha creado el primer Equipo de Respuesta ante Emergencias Informáticas (CERT) especializado en infraestructuras críticas, de las que el 80% son empresas privadas. A nivel estatal, el Centro Criptológico Nacional, encuadrado en el CNI, es el responsable de gestionar la seguridad del ciberespacio en cualquiera de los tres niveles de la Administración, y dispone de un Equipo de Respuesta ante Emergencias Informáticas (CERT).

4 MARCO CONCEPTUAL

La protección del ciberespacio es esencial para preservar la seguridad y defensa de la nación y su economía, por lo tanto, la adopción de una Política Nacional de Ciberseguridad y Ciberdefensa que involucre a todos los sectores de la sociedad, bajo el liderazgo del Ministerio de Defensa Nacional en coordinación con los demás entes del Estado, es un imperativo al que debe darse la mayor de las prioridades.

El delito cibernético contempla desde el acceso abusivo a un sistema informático, el diseño y propagación de código malicioso (virus), la pornografía infantil, el uso de la tecnología para fines delictivos como el hurto, la estafa y el tráfico de drogas, hasta la amenaza a la seguridad de los sistemas financieros, servicios públicos y demás infraestructuras críticas para cualquier Estado.

Es un delito dinámico que se vale de un supuesto anonimato para atentar contra la confidencialidad, integridad y disponibilidad de la información. Se ha constituido, aprovechando la importante expansión de las tecnologías de la información y las comunicaciones, en un delito transnacional que plantea retos importantes a las autoridades en la labor de prevención, reacción, investigación y judicialización.

En consecuencia, es necesario basar la lucha contra las amenazas a la Ciberseguridad y Ciberdefensa, en la cooperación nacional e internacional para el intercambio de información y mejores prácticas, como también aunar esfuerzos en todos los sectores del país tendientes a desarrollar una estrategia nacional de Ciberseguridad y Ciberdefensa que permita proteger la infraestructura critica del país y disponer de capacidades de contención y reacción.

Los lineamientos para el desarrollo e impulso de la Ciberseguridad y Ciberdefensa consisten en la estructuración y articulación de las capacidades y mecanismos coordinados por el gobierno nacional con el fin de identificar y establecer acciones y responsabilidades tendientes a prevenir, preparar, controlar, recuperar y responder frente a todo tipo de incidentes o amenazas cibernéticas a las que puede estar expuesto el país.

Con el fin de lograr los objetivos propuestos es necesario involucrar todos los sectores e instituciones del Estado con responsabilidad en el campo de Ciberseguridad y Ciberdefensa. Igualmente, es de vital importancia crear conciencia y sensibilizar a la población en todo lo referente a la seguridad de la información.

Así mismo, se debe fortalecer los niveles de cooperación internacional en aspectos de Ciberseguridad y Ciberdefensa que permitan la integración, colaboración y cooperación con organismos dedicados a este mismo fin.

5 DIAGNÓSTICO

Como consecuencia de los cambios tecnológicos, la confidencialidad, integridad, disponibilidad en la transmisión, procesamiento, almacenamiento y uso de la información exige altos niveles de seguridad. Adicionalmente, la introducción de las redes globales de comunicaciones ha generado a su vez nuevos ambientes para vulnerar, comprometer y modificar la información.

Los beneficios de las redes de comunicaciones (voz y datos) son ilimitados, sin embargo día a día nos enfrentamos a nuevas y cada vez más complejas amenazas informáticas que se presentan de formas nunca antes vistas, lo cual exige a su vez, la creación de nuevos mecanismos de prevención, reacción y defensa.

Países como Estados Unidos, Brasil, Argentina, Uruguay (entre otros), ya han tomado conciencia de esta necesidad y han organizado sus propios equipos para atender y responder proactivamente a cualquier incidente cibernético, como se muestra en los siguientes mapas:

Gráfica1. Equipos de Respuesta a Incidentes alrededor del mundo. Tomado de: CERT/CC

En la siguiente tabla, se muestran las páginas web donde se pueden encontrar las diferentes directrices sobre penalización contra delitos cibernéticos en países como Japón, Estados Unidos, Inglaterra, Alemania, Canadá, Italia y Francia.

Tabla 1. Directrices Internacionales sobre delincuencia cibernética

	CERT	FORTALECIMIENTO DE LA LEY
CANADA	http://www.ocipep.gc.ca	http://www.rcmp-grc.gc.ca
FRANCIA	http://www.certa.ssi.gouv.fr	http://interieur.gouv.fr/rubriques/c/c3_police_nationale/c33;2_oclctic
ALEMANIA	http://www.bsi.de	http://www.bmi.bund.de
ITALIA	http://idea.sec.ds.unimi.it	http://www.poliziadistato.it/pds/informatica
JAPON	http://www.jpcert.or.jp http://www.npa.go.jp/cyber http://www.ipa.go.jp/security	http://www.npa.go.jp/cyber
INGLATERRA	http://www.niscc.gov.uk	http://www.nhtcu.org
ESTADOS UNIDOS	http://www.us-cert.gov	http://www.cybercrime.gov/reporting.htm

Tomado de: Información Relevante para la implementación de una Estrategia Nacional de Ciberseguridad CRC

En el aspecto de defensa y seguridad, se observa la incorporación de nuevas capacidades tecnológicas a nivel internacional y la activación de organismos con propósitos definidos de Ciberseguridad y Ciberdefensa, como se muestra en la siguiente tabla:

Tabla 2. Capacidades tecnológicas a nivel internacional

PAÌS	ACCIÓN TOMADA POR EL GOBIERNO
ESTADOS UNIDOS	Creó un Centro de Ciber-Comando Unificado que depende de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés).
AUSTRALIA	Creó el Centro de Operaciones Cibernéticas que coordina las acciones estatales ante los incidentes ocurridos en el ciberespacio.

CHINA	Tiene una capacidad bien conformada y hombres entrenados dentro del Comando Cibernético Conjunto (militar y civil).
ESTONIA	En 2008 creó conjuntamente con otros países de Europa, la OTAN y EE.UU. el Centro Internacional de Análisis de Ciberamenazas.
FRANCIA	Creó la Agencia de Seguridad para las Redes e Información (FINSA), que vigila las redes informáticas gubernamentales y privadas con el fin de defenderlas de ataques cibernéticos.

Tomado de: Dirección de Estudios Sectoriales Ministerio de defensa Colombia

Las entidades colombianas (tanto privadas como gubernamentales) vienen concientizándose de la importancia de fortalecer los aspectos de seguridad de la información en las áreas de infraestructuras propias y compartidas de conectividad.

De acuerdo con un estudio realizado en Marzo de 2010, por la Guardia Civil Española en colaboración con el FBI y la empresa de antivirus Panda Security se desmanteló una red de computadores "zombies" conocida bajo el nombre de 'BotNet Mariposa', la cual dio mucho de qué hablar al ser esta una de las mayores redes de PCs zombies del mundo desarticulada hasta el momento, estaba compuesta por más de 13 millones de direcciones IP (Protocolo de Internet) infectadas, distribuidas en 190 países alrededor del mundo, así:

Tabla 3. Top 20 de países más afectados

PAÍS	%
INDIA	19.14
MÉXICO	12.85
BRASIL	7.74
COREA	7.24
COLOMBIA	4.94
RUSIA	3.14
EGIPTO	2.99
MALASIA	2.86
UCRANIA	2.69
PAKISTAN	2.55
PERU	2.42
IRAN	2.07
ARABIA SAUDI	1.85
CHILE	1.74
KAZAKHSTAN	1.38
EMIRATOS ARABES	1.15
MARRUECOS	1.13
ARGENTINA	1.10
ESTADOS UNIDOS	1.05

Tomado de: www.infospyware.com

El aumento en la penetración de internet en Colombia ha provocado paralelamente el incremento en el uso de servicios electrónicos ofrecidos sobre ese medio de comunicación, el cual se ha convertido en una oportunidad para brindar acceso a mayor población. Dado lo anterior y todos los beneficios que conlleva la utilización del Internet, igualmente aumenta el "campo de acción" para los atacantes informáticos.

En la siguiente gráfica se aprecia el crecimiento de uso de internet en Colombia en un periodo de un año del tercer trimestre de 2013 al tercer trimestre de 2014:

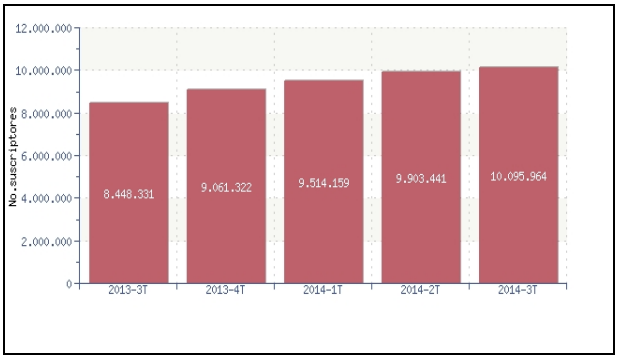


Gráfico 2. Total de suscriptores de internet. Tomado de: MINTIC-SIUST

5.1 Problemática

5.1.1 Problema central

A pesar de existir diversas iniciativas normativas y de política en el país en torno a la temática de Ciberdefensa y Ciberseguridad nacional, y los avances generados a nivel de infraestructura de telecomunicaciones, la capacidad del Estado para enfrentar las amenazas que atentan contra la Ciberseguridad y Ciberdefensa nacional es insuficiente.

5.1.2 Efectos del problema central

-Debilidad en la normatividad para la regulación de los ISPs (Proveedores de Servicios de Internet).
-Para temas de investigación judicial no se guardan Logs (registros de auditoría) de eventos por un tiempo adecuado.
-Débil sistema de verificación de datos en la asignación de licencias de operación y prestación de servicios.
-Incremento de la impunidad.
-Incremento de delincuencia cibernética.
-Incremento del riesgo.
-Inadecuado manejo de la evidencia digital.
-Rezago del país ante la comunidad internacional en Ciberseguridad y Ciberdefensa.

5.1.3 Ejes problemáticos

Se identifican tres (3) ejes problemáticos:

1. Debilidad en la cobertura de capacitación especializada en Ciberdefensa y Ciberseguridad

Aunque en el país existen algunas instituciones de educación superior que ofrecen especializaciones de seguridad y derecho informático, se ha identificado la debilidad en el número y en la oferta de estas instituciones para brindar programas en estos temas, el cual como mínimo debería ser a nivel de maestría. Adicionalmente, se considera que el conocimiento acerca de la seguridad de la información, Ciberseguridad y Ciberdefensa es deficiente en el sector público y privado. Las personas que acceden a algún tipo de formación en el área de seguridad lo hacen mediante algunas certificaciones de carácter internacional que no son transversales en el conocimiento requerido y formaciones de carácter de maestría solo están al alcance de manera virtual donde la mayoría de las veces se estudian entornos diferentes al colombiano.

2. La coordinación de las estrategias y las operaciones de Ciberseguridad y Ciberdefensa se encuentran desatendidas

A pesar de existir algunos esfuerzos institucionales (tanto privados como públicos) se evidencia que no existen organismos a nivel nacional para coordinar y desarrollar operaciones de Ciberseguridad y Ciberdefensa. Por lo tanto, no ha sido posible establecer los mecanismos suficientes y adecuados para contrarrestar ataques cibernéticos y proteger los intereses del Estado en el ciberespacio; así mismo, no se cuenta con medidas suficientes para afrontar ataques cibernéticos que atenten contra las infraestructuras críticas de la nación.

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

La protección del ciberespacio requiere la actualización de las leyes penales, los procedimientos y las políticas deben hacer frente y responder oportunamente a los ataques de la delincuencia cibernética. Para esto es necesario promulgar y aplicar un amplio conjunto de leyes relativas a la Ciberseguridad y Ciberdefensa.

Se evidencia que no existe una regulación adecuada en cuanto al compromiso que deben tener todos los ISPs con referencia a la preservación de Logs para que sirvan en determinado momento como prueba o contribuyan en las investigaciones de delitos cibernéticos.

6 OBJETIVOS

6.1 Objetivo Central

Fortalecer la capacidad del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (Ciberseguridad y Ciberdefensa), creando el ambiente y las condiciones necesarias para brindar la protección en el ciberespacio y de las infraestructuras críticas nacionales.

6.1.1 Objetivos específicos

-Diseñar e implementar planes y programas de capacitación en seguridad de la información en instituciones de educación superior.
Este objetivo permitirá generar conocimiento especializado en esta materia para afrontar las amenazas que atentan contra la confidencialidad, integridad y disponibilidad de la información.
-Implementar instancias apropiadas para atender, controlar y generar recomendaciones que regulen los incidentes y/o emergencias cibernéticas para proteger las infraestructuras críticas nacionales.
Este objetivo permitirá al Estado mejorar su capacidad para afrontar las amenazas y los riesgos que atentan contra la Ciberseguridad y Ciberdefensa nacional.
-Fortalecer la legislación en materia de Ciberdefensa y Ciberseguridad.
Este objetivo permitirá al Estado brindar las herramientas jurídicas necesarias para la prevención, investigación y judicialización de los ciberdelitos.
-Incrementar la capacidad de los organismos de seguridad del Estado para enfrentar las amenazas informáticas que atenten contra la Defensa Nacional.
Este objetivo permitirá a los organismos de seguridad del Estado conformar organismos interinstitucionales con la capacidad técnica y operativa necesaria para la Defensa Nacional.

7 CREACIÓN DE UNA UNIDAD DE CIBERDEFENSA Y/O CIBERSEGURIDAD EN LA ENTIDAD

7.1 Ciberseguridad

Centrada en la defensa y protección de sus redes frente a intrusiones de las mismas en el ciberespacio. Incluye tanto medidas preventivas como reactivas.

Su ámbito lo compone:
-Incidentes tanto fortuitos como maliciosos.
-Comprende ciberataques y los desastres naturales.
-Aborda el ciclo de vida entero del sistema.

7.2 Ciberdefensa

Subconjunto de la anterior, que tiene lugar en la fase operativa y se materializa mediante los ciberataques y su defensa.

Su ámbito lo compone:
-Incidentes con propósito malicioso.
-Comprende sólo ciberataques.
-Presente sólo en la fase de operación de sistema CIS.

7.3 Ciclo de la ciberdefensa

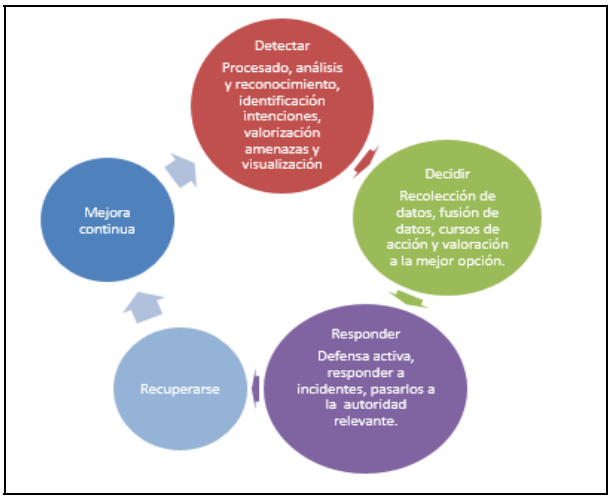
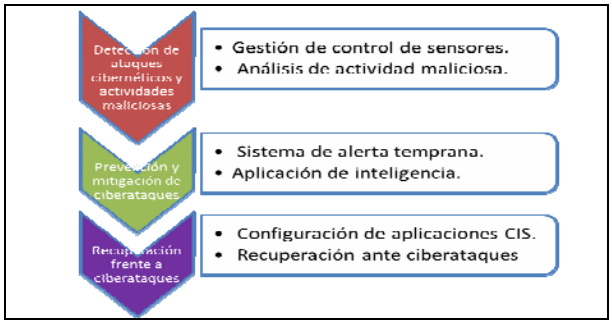
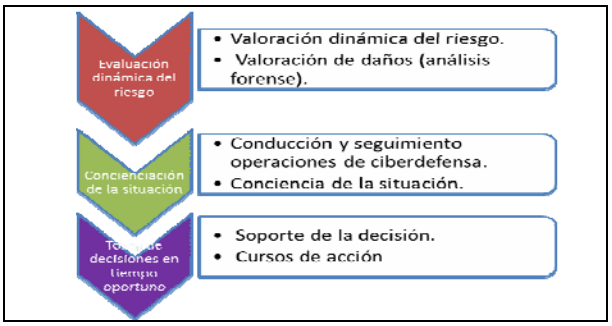


Gráfico 3. Ciclo de la Ciberdefensa. Tomado de: Ejército Nacional de Colombia. Unidad de Ciberdefensa.

7.4 Capacidades en ciberdefensa





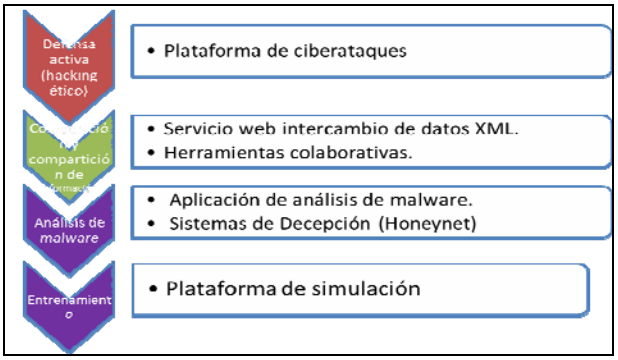


Gráfico 4. Capacidades de la Ciberdefensa. Tomado de: Ejército Nacional de Colombia. Unidad de Ciberdefensa.

7.5 Capas en ciberdefensa

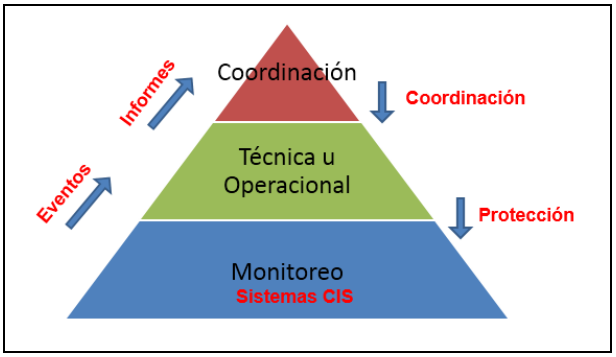


Gráfico 5. Capas de la Ciberdefensa. Tomado de: Ejército Nacional de Colombia. Unidad de Ciberdefensa.

7.6 Funciones de las capas

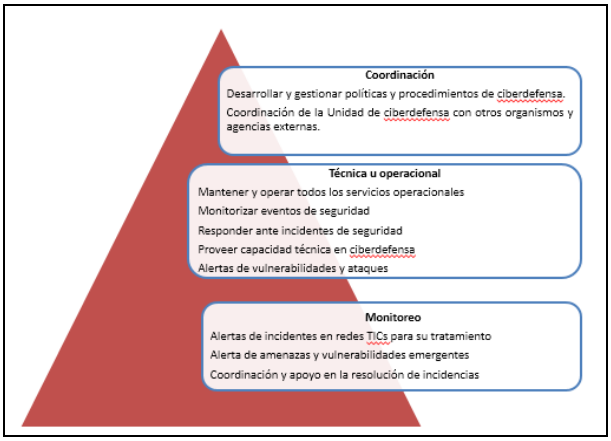


Gráfico 6. Funciones de las Capas. Tomado de: Ejército Nacional de Colombia. Unidad de Ciberdefensa.

8 CONCLUSIONES

Millones de personas utilizan los servicios y la información que les provee el Ciberespacio, generando una inmensa y creciente dependencia. Sin embargo, La Ciberdefensa y Ciberseguridad es un tema al cual no se le da la importancia que merece y que es desconocido por muchos. Es por ello, que se debe sensibilizar la población por parte de las instituciones directamente relacionadas, tal y como se muestra en las gráficas de Ejército Nacional. Es muy importante tener una estrategia de Ciberdefensa y Ciberseguridad que este alineada con los propósitos del sector defensa y cumpla con toda la normatividad indicada.

Por otro lado es importante que se le preste explicita atención a los cambios tecnológicos que se ven hoy en día lo que permite que los ataques Cibernéticos sean cada vez más complejos y la infraestructura cada vez más crítica. Sin embargo, esto se puede mitigar con la política de Ciberseguridad y Ciberdefensa que tiene el gobierno Colombiano y su correcta aplicación.

En Colombia se tiene una gran plataforma tecnológica y una política bien estructurada la cual ha tenido mayor acogida en los últimos años, pero, es importante recordar que el sector debe amoldar el tema jurídico y lograr un mayor control sobre las entidades que realizan este tipo de actividades, logrando así reducir el índice de vulnerabilidades que pueden llegar a tener el sector y de esta manera se puede prevenir ataques y brindarle seguridad a todo un país.

9 REFERENCIAS

[1] Comisión interamericana de telecomunicaciones. Boletín electrónico / (Número 1 - Julio, 2004). [En línea]. Disponible en: http://www.oas.org

[2] Convenio sobre Cibercriminalidad. (2001, Nov 23). [En línea]. Disponible en: http://conventions.coe.int

[3] Política de Seguridad Externa Común Decisión 587. (Julio de 2004). [En línea]. Disponible en: http://www.comunidadandina.org

[4] Delito Cibernético. [En línea]. Disponible en: http://programa.gobiernoenlinea.gov.co

[5] The CERT Division. [En línea]. Disponible en: www.cert.org

[6] Agenda Regulatoria 2015-2016 - CRC. [En línea]. Disponible en: www.crcom.gov.co

[7] Total de suscriptores de internet. MINTIC-SIUST. [En línea]. Disponible en: www.vivedigital.gov.co

[8] Documento Conpes. Lineamientos de política para el desarrollo e impulso de la Ciberdefensa y Ciberseguridad.