CIBERSEGURIDAD Y CIBERDEFENSA EN COLOMBIA.

Camacho L. Reinerio. Amaya A. Alexis J.
79’616.227. - 17’593.911.
Rcamachol1973@hotmail.com – Jovanny25@hotmail.es
Universidad Piloto De Colombia.

Resumen – El presente artículo de investigación tiene como objetivo mostrar los lineamientos adoptados de Ciberseguridad y Ciberdefensa, para la gestión, protección, procesamiento, almacenamiento y transmisión de datos e información; a través de Tecnologías de Información y Comunicaciones (TIC). Así como el rol que desempeña la informática forense en la Seguridad Nacional, tal como se ha declarado y planteado en diversos textos diseñados por diferentes entes del sector público y privado y la relación de estos temas identificando que hay, que falta y cómo vamos en materia de Informática Forense. Finalmente, estaremos en capacidad de conocer el estado actual de seguridad informática, Ciberseguridad y Ciberdefensa y que se tiene en materia especifica de Informática Forense.

Índice de Términos **- Ciberseguridad, Ciberdefensa, Ciberterrorismo, Ciberdelitos, Forense,Infraestructura critica.**

I. INTRODUCCION

Las tecnologías al ser aplicadas en distintos campos de acción, ha logrado posicionarse en diferentes sectores de la economía, hasta hace un par de décadas se realizaban tareas netamente manuales. Al haberse realizado esta evolución de lo manual a lo tecnológico, no solo se han obtenido ventajas y desventajas, sino también se han adquirido factores de riesgo, convirtiéndose en amenazas y vulnerabilidades que ameritan un cuidado especial y un tratamiento integral.

Un ejemplo de aplicación de tecnologías modernas, son implementación de las tecnologías de información y telecomunicaciones, en aplicaciones electrónicas de control, administración y gestión en infraestructura critica, convirtiéndose en puntos claves para la economía de un país, y al mismo tiempo en objetivos estratégicos, para la realización y ejecución de Ciberdelitos.

En Colombia, solo desde el año 2005, nos empezamos a preocupar por las amenazas y vulnerabilidades tanto internas como externas de origen cibernético; uniendo esfuerzos inter institucionales y generando lineamientos que permitan prevenir, contrarrestar y atender estos flagelos mediante una política global de “Ciberseguridad” y “Ciberdefensa”.

Estos esfuerzos incluyen la creación de leyes en protección de datos, lineamientos para alinear a las instituciones encargadas de la Seguridad Nacional y proveer de herramientas que permitan generar

estrategias de prevención y mitigación de riesgos y amenazas, provenientes del ciberespacio, que pretendan generar caos nacional y desestabilizar la economía del país.

El presente artículo pretende mostrar los lineamientos y políticas adoptadas para "Ciberseguridad" y "Ciberdefensa" y el rol intrínseco que desempeña la Informática Forense.

II. CIBERSEGURIDAD Y CIBERDEFENSA EN INFRAESTRUCTURA CRÍTICA DEL PAIS. [1].

En Colombia, las instituciones públicas y privadas se han interconectado al ciberespacio, convirtiéndose en parte vital en el cumplimiento de sus funciones y actividades asignadas, pero también ha traído consigo mismo, muchos problemas de seguridad informática, permitiendo un incremento en delitos informáticos, que afectan la estabilidad y el funcionamiento del país, impactando directamente en los activos críticos de infraestructura, siendo esta una de las grandes preocupaciones.

El sector energético es uno de esos pilares de la economía nacional, y lleva buen ritmo de modernización tecnológica y sistematización de sus procesos que intervienen en la generación, transmisión y distribución de energía eléctrica. Incorporando nuevas tecnologías de automatización en centros de gestión, con infraestructura tecnológica y arquitecturas de comunicaciones, su implementación incrementó de manera sustancial, las amenazas y riesgos en el ciberespacio, afectando la integridad, confidencialidad y disponibilidad de la información; Así mismo, se pone en evidencia la variedad de amenazas cibernéticas tales como; sabotaje en servicios y terrorismo informático, entre otras, bien sean internas o externas que afectarían el suministro eléctrico del país.

Teniendo en cuenta lo anterior, se han generado lineamientos y políticas para la gestión de la infraestructura tecnológica crítica, información pública y privada, "Ciberseguridad" y "Ciberdefensa". Permitiendo a las instituciones implementar normas que garanticen las buenas prácticas en lo relacionado a la seguridad de sus procesos. El consejo nacional de operación "C.N.O", elaboró una "GUÍA DE CIBERSEGURIDAD"[1], la cual está dirigida al consejo nacional de operación, operador del sistema, generadores, transmisores y distribuidores de Energía.

En la actualidad se desconoce el avance y la aplicación de esta guía, y las medidas que han adoptado las empresas de distribución de energía para afrontar la gran variedad de delitos informáticos, ataques cibernéticos y si cuentan o no con unidades responsables para la planeación, coordinación y administración de incidentes en delitos informáticos y

[1] Documento COMPES 3701: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Ciberterrorismo, bajo procedimientos prácticos asociados con respuesta a incidentes, incluyendo la recolección y obtención de datos y el análisis de los mismos contenidos en medios de almacenamiento tecnológicos, de tal forma que su información pueda ser utilizada como evidencia probatoria ante un ente judicial o autoridad respectiva demostrando la responsabilidad sobre un hecho cuyas sanciones podrían llevar a ser penales y/o administrativas.

III. SECTOR ELECTRICO EN COLOMBIA. [2].

Las empresas distribuidoras o comercializadoras, según "ASOCODIS": "Representan un segmento clave dentro de la industria colombiana, ya que son responsables de suministrar el servicio de energía eléctrica a 8.9 millones de usuarios que representan el 98.5% de los usuarios de Colombia, y de atender el 97% de la demanda de energía regulada del país"[2].

Según estas cifras y lo planteado en lo que va de este artículo, es fácil de apreciar la importancia que tiene la adopción e implementación de esta "GUÍA DE CIBERSEGURIDAD", su adaptación a cada empresa y el impacto que tendría, en caso de materializarse un ataque a través del ciberespacio en contra de los activos críticos de la infraestructura del sector eléctrico.

[2] ASOCODIS. Asociación Colombiana de Distribuidores de Energía Eléctrica.

Las empresas distribuidoras, tiene como misión, disponer y proveer de energía eléctrica suficiente en todo momento a través de sistemas de generación, transmisión y distribución de energía eléctrica para soportar la economía del país, siendo este uno de los servicios más importantes y como tal, requiere de una protección adecuada y la seguridad de la información protege a ésta de un amplio espectro de amenazas, a efectos de asegurar la continuidad del servicio, minimizando sus daños y maximizando el retorno de inversiones.

Los cambios tecnológicos y la modernización implementada en el sector eléctrico, se ha visto abordado por gran variedad de amenazas provenientes del ciberespacio, teniendo en cuenta la complejidad y la importancia del sector eléctrico para la economía del país, debemos preguntarnos en qué medida y que tan avanzado es el aseguramiento de la infraestructura eléctrica, con respecto a la aplicación de normas y buenas prácticas en materia de "Ciberseguridad" y "Ciberdefensa".

Por lo anterior, se ha modernizado la infraestructura tecnológica del sector, permitiendo que los procesos de generación, transmisión y distribución, se lleven a cabo con la mayor efectividad y seguridad, garantizando que el servicio se preste con la mayor calidad posible, con fluido continúo y sin inconvenientes, apagones, racionamientos, sabotajes, etc., que deterioren o perjudiquen los demás sectores económicos del país.

La utilización de tecnología informática, es un proceso de modernización que como cualquier otro proceso de cambio, trae sus ventajas y desventajas. Al pasar de tecnologías cerradas a tecnologías abiertas e interconectadas, se corren riesgos a "Ataques Informáticos" o "Ciberataques". Un ataque que logre impactar y neutralizar una sub estación, no solo afecta la economía de quienes hacen uso de este servicio, sino que se convierte en una onda expansiva que crece en todas direcciones, logrando proporciones en ocasiones difíciles de calcular en términos financieros, e impactando de manera negativa, en las actividades económicas de un país, interrupción en la prestación del servicio, el cual se mide en el binomio (kilovatio/hora), aumentando los costos por compensación y afectando los indicadores de calidad en la prestación del servicio y otros traumatismos de índole económicos y pérdidas financieras,

La aplicación de normas de "Ciberseguridad" y "Ciberdefensa" en cualquier sector, no solo está orientada a prevenir los ataques de los Ciberdelincuentes, sino a que las instituciones y/o empresas se puedan recuperar, en forma rápida y eficaz de cualquier incidente, que altere o impacte de manera negativa las operaciones de las mismas. Algunos incidentes pueden ser causados por error humano y de procedimientos.

IV. ANTECEDENTES A NIVEL MUNDIAL. [3].

El presente artículo pretende mostrar los lineamientos y políticas adoptadas en "Ciberseguridad" y "Ciberdefensa", identificando la situación actual y aplicación de cada uno de los criterios establecidos en las diferentes normas que se han diseñado, específicamente en empresas distribuidoras de energía y recurrir a las experiencias de diferentes países en materia de delitos Informáticos.

Recientemente una encuesta a 200 ejecutivos de seguridad de TI de empresas de infraestructura del sector eléctrico en 14 países mostro que el 40% de los ejecutivos pensaba que la vulnerabilidad del sector había aumentado. Casi el 30% opinó que su empresa no estaba preparada para enfrentar un ataque cibernético y más del 40% tiene previsto que su empresa enfrente un ataque cibernético importante dentro del año próximo.

De acuerdo a todo lo anterior, su evolución y el flagelo de la inseguridad informática, sofisticación de los ataques informáticos, sus estadísticas y la creciente ola de ataques a infraestructuras críticas para diferentes países y empresas, se mencionan algunos de los más relevantes de la historia:

- ✓ En abril del 2007, el gobierno de estonia sufrió el que es considerado el mayor ataque cibernético de la historia, en el cual se vieron afectados la presidencia, el

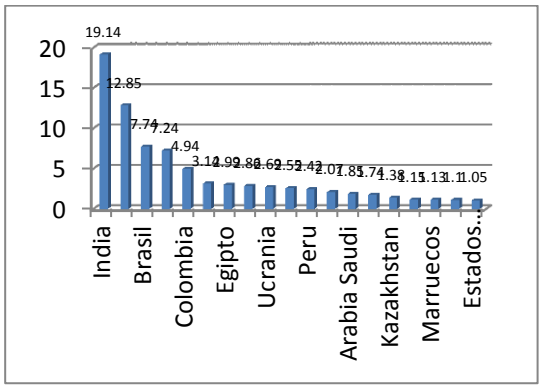
parlamento, los ministerios y dos de sus grandes bancos.

- ✓ En contra de los Estados Unidos en julio de 2009, una serie de ataques afectaron la casa blanca, el departamento de seguridad interna (DHS), el departamento de defensa, la administración federal de aviación y la comisión federal de comercio.
- ✓ La Guardia Civil española en marzo de 2010, desmanteló a una de las mayores redes de computadores "zombis", conocida con el nombre de 'BootNet Mariposa', compuesta por más de 13 millones de direcciones IP infectadas, distribuidas en 190 países alrededor del mundo. Colombia ocupó el quinto puesto entre los países más afectados por esta red.

País	%
INDIA	19.14
MÉJICO	12.85
BRASIL	7.74
COREA	7.24
COLOMBIA	4.94
RUSIA	3.14
EGIPTO	2.99
MALASIA	2.86
UCRANIA	2.69
PAKISTÁN	2.55
PERÚ	2.42
IRÁN	2.07
ARABIA SAUDÍ	1.85
CHILE	1.74
KAZAKHSTÁN	1.38
EMIRATOS ÁRABES UNIDOS	1.15
MARRUECOS	1.13
ARGENTINA	1.10
ESTADOS UNIDOS	1.05

Tabla N° 2: Top 20 de países afectados por BootNet Mariposa.

"Latinoamérica encabeza el Top 20 en países más afectados, conformados por: **México**, con el 12,85%, **Brasil**, con el 7,74%, **Colombia**, con el 4,94%, **Perú**, con el 2,42%, **Chile**, con el 1,74%, y **Argentina**, con el 1,10% del total."[3]



V. COMBATIENDO EL CIBER TERRORISMO. [4].

Desde el año 2005, el Ministerio de Relaciones Exteriores creó un grupo interdisciplinario de trabajo para analizar y profundizar en temas concernientes al ciberespacio. Posteriormente, el Ministerio de Tics, por medio de una consultoría, identifico las brechas y los vacíos que tiene la nación en materia de Seguridad Informática.

Teniendo como resultado de esta iniciativa y el de múltiples discusiones en el grupo de trabajo, la cancillería, el ministerio del interior y justicia, el ministerio de Tics, y otras entidades involucradas en el proceso, decidieron que el ministerio de defensa liderara los temas de "Ciberseguridad" y "Ciberdefensa". Como resultado más significativo que ha tenido este grupo de

[3]Cifras tomadas de Info Spyware. Disponible en:http://www.infospyware.com/blog/latinoamerica-dentro-de-los-mas-afectados-por-la-botnet-mariposa/

trabajo, ha sido la creación, en el 2009 "COLCERT" (Grupo de Respuesta a Emergencias Cibernéticas de Colombia), cuya función es coordinar las acciones necesarias para la protección de la infraestructura critica del país, frente a las emergencias de amenazas cibernéticas que atenten o comprometan la seguridad y defensa nacional.

El 13 de diciembre de 2007, la comisión de regulación de telecomunicaciones publicó para conocimiento del sector y en general, un documento que entrega al gobierno nacional, sector privado y la academia recomendaciones para la creación de una estrategia nacional de "Ciberseguridad", y a su vez proporcionar instrumentos idóneos para la colaboración y cooperación entre el gobierno y todos los niveles del sector privado, identificando caminos para la disuasión del crimen cibernético, recomendando la implementación y desarrollo de marcos jurídicos relacionados con la "Ciberseguridad" que sean consistentes con los parámetros internacionales y la elaboración de sistemas de respuesta ante incidentes de seguridad en la red, incluyendo la vigilancia, análisis y respuesta a estos incidentes y proponer lineamientos para la implementación de una cultura nacional de "Ciberseguridad" que mejore los niveles de protección de las infraestructuras críticas del país.

El ministerio de las tecnologías de información y las comunicaciones, redactó y publicó un modelo de seguridad de la información para la estrategia de gobierno en línea (GEL), en el marco del programa gobierno en línea. **[5].** Este modelo de seguridad hace referencia al conjunto de políticas estratégicas que soportan objetivos de gobierno en línea como la "Protección de información del individuo" y la "credibilidad y confianza en el gobierno en línea". Establece como elementos fundamentales de la seguridad de la información para los organismos gubernamentales:

- ✓ La disponibilidad de la información y los servicios.
- ✓ La integridad de la información y los datos.
- ✓ Confidencialidad de la información.

De otra parte, fue creado también el "CSIRT-CCIT", es un centro de coordinación de atención a incidentes de seguridad informática, el cual está en contacto directo con los centros de seguridad de empresas afiliadas y está en capacidad de coordinar el tratamiento y la solución de solicitudes y denuncias sobre problemas de seguridad informática que sean recibidas a través de una cuenta de correo electrónico. Actualmente se están efectuando trabajos en contra del robo de información privada (Phishing), la cual es usada posteriormente para sustraer dinero de las cuentas bancarias de las víctimas.

El gobierno nacional en el año 2011, inició el desarrollo de lineamientos y políticas para "Ciberseguridad" y "Ciberdefensa", logrando incluir este

tema en el plan nacional de desarrollo 2010-2014. **[6].**

Estos lineamientos van dirigidos a proteger la infraestructura crítica y sectores claves para la estabilidad del país, como son; el ministerio de interior y de justicia, el ministerio de relaciones exteriores, el ministerio de defensa nacional, el ministerio de tecnologías de la información y las comunicaciones, el departamento administrativo de seguridad, el departamento nacional de planeación y la fiscalía general. Buscando que se convierta en el mecanismo que permita el desarrollo de políticas de prevención y control de los riesgos y las amenazas derivados del incremento del uso de las tecnologías y en general los delitos del ciberespacio.

Basados en las iniciativas expuestas anteriormente y en el documento "CONPES 3701", el cual provee los lineamientos generales para el desarrollo de la temática de protección de la infraestructura crítica del país, el consejo nacional de operación "C.N.O.", a través de su grupo tecnológico, elaboraron la "GUÍA DE CIBERSEGURIDAD" aplicable al sector eléctrico Colombiano. **[7].**

Teniendo en cuenta, la evolución tecnológica que le sector ha sufrido, orientado a garantizar la confiabilidad y estabilidad de los sistemas de potencia y transmisión nacional y regional, esta guía toma como referencia las normas NERC[4] CIP[5] -002 a la CIP -009, normas americanas que fueron adaptadas para el sistema eléctrico colombiano. Estas normas de referencia, tratan temas como la definición de Ciberactivos críticos, controles en la gestión de seguridad de la información, personal y entrenamiento, perímetros de seguridad electrónica, seguridad física, gestión de la seguridad, reportes de incidentes y planes de respuestas y recuperación para Ciber activos críticos.

VI. ESTRATEGIA DE CIBERSEGURIDAD Y CIBERDEFENSA. [8].

El 14 de Julio de 2011, el Ministro De Defensa Nacional, Doctor Rodrigo Rivera, presentó a la opinión pública la estrategia integral de "Ciberseguridad" y "Ciberdefensa"; de la siguiente manera: [6]

"Colombia ya hace parte de un grupo muy pequeño de países que hasta este momento han adoptado una estrategia de ésta naturaleza, integral, comprensiva, que involucra todos los matices, las aristas, para enfrentar retos de "Cibercrimen", que puedan darse en el ciberespacio, pero también retos de

[4] NERC: North American Electric Reliability Corporation.

[5] CIP: Critical Infrastructure Protection.

[6] Fragmentos extraídos de las declaraciones del Ministro de la Defensa Nacional, Doctor Rodrigo Rivera, en la presentación de la estrategia de Ciberseguridad y Ciberdefensa. Disponible en: http://www.mindefensa.gov.co/irj/go/km/docs/documents/News/NoticiaGrandeMDN/60a20bd2-8890-2e10-7dab-8a117a5461d8.xml

"Ciberdefensa", es decir los riesgos de afectación de infraestructura sensible"

"Tras su aprobación por parte del Consejo Nacional de Política Económica y Social "CONPES", esta nueva estrategia del Gobierno Nacional y la Fuerza Pública, crea tres (3) grupos orientados a proteger a los cibernautas y los sistemas de información nacional"

"i) El Grupo de Respuesta a Emergencias Cibernéticas de Colombia "COL-CERT", que tendrá como misión la coordinación de la gestión de emergencias de "Ciberseguridad" que puedan afectar la infraestructura central nacional".

"ii) El Comando Conjunto Cibernético de las Fuerzas Militares, que tendrá responsabilidad de salvaguardar los intereses nacionales en el ciberespacio.

iii) El Centro Cibernético Policial, que estará a cargo de la prevención, la investigación y apoyará la judicialización de los delitos informáticos. Para ello, contará con un Comando de Atención Inmediata Virtual "CAI-VIRTUAL" para recibir las denuncias de los ciudadanos".

"Además, habrá una Comisión Intersectorial encabezada por el Presidente de la República, integrada por los ministros de Defensa, de Tecnologías de la información, el Alto Consejero para la Seguridad, los directores del DAS y del Departamento de Planeación".

La estrategia de "Ciberseguridad" y "Ciberdefensa", estará liderada por la comisión intersectorial, apoyando su gestión en los tres (3) grupos de respuesta a incidentes de "Ciberseguridad". Es así como el "COL-CERT", El Comando Conjunto Cibernético de las Fuerzas Militares y el Centro Cibernético Policial, ejercerán acciones que permitan la colaboración activa en la resolución de incidentes. Para resolver estos incidentes, el centro cibernético policial, adopta una serie de acciones a realizar, estas son: **[9].**

- ✓ Respuesta en línea a incidentes de "Ciberseguridad" Cuadrante Virtual – "CAI-VIRTUAL".
- ✓ Coordinación Internacional INTERPOL EUROPOL - Grupo de Trabajo de Delitos Tecnológicos.
- ✓ Atención de incidentes informáticos DIJIN - Laboratorios móviles de informática forense.
- ✓ Implementación "CSIRT-PONAL" (Equipo de Respuesta a Incidentes Informáticos de la Policía Nacional).
- ✓ Laboratorio de investigación de malware - (Sector Bancario).
- ✓ Análisis forense equipos - Tablet Mac-Servidores-Smarth Phones.
- ✓ Atención, Judicialización de incidentes Cibernéticos (Afectación en distintos niveles y sectores).
- ✓ Unidades de investigación tecnológica UDITE (44) - Cobertura nacional de la problemática.

Estas actividades tienen como eje fundamental, la informática forense, a través de la implementación de laboratorios móviles para análisis forense con equipos de cómputo y de telecomunicaciones.

Por su parte el comando conjunto cibernético se encargara de la implementación de la estrategia de la siguiente manera:

- ✓ **Fase I**: Año 2012. Monitoreo, Análisis de Vulnerabilidades, Capacitación Nivel I y Formación Estrategia.

- ✓ **Fase II**: Año 2013. Alertas tempranas, Monitorización del Riesgo, Correlación Compleja, Tratamiento y respuestas a Incidentes, Operaciones de Ciberdefensa, Capacitación Nivel II, Concienciación y Cooperación Internacional.
- ✓ **Fase III**: Año 2014. Análisis Forense Básico, Operaciones de Ciberdefensa, Operaciones de Inteligencia, Auditorias y Evaluaciones Seguridad, Aseguramiento de Portales FF.MM, Capacitación Especializada en Ciberseguridad y Ciberdefensa, Cooperación Internacional y Membrecía al FIRST.
- ✓ **Fase IV**: Año 2015. Construcción Infraestructura (TOE), Ciberoperaciones Especiales, Desarrollo de Herramientas de Seguridad, Pagina CSIRT FF.MM y Capacitación.
- ✓ **Fase V**: Año 2016. Ciberdefensa, Infraestructura Critica Nacional, Laboratorios análisis forense, Laboratorios criptoanálisis y Capacitación.
- ✓ **Fase VI**: Año 2017. Laboratorios de análisis y desarrollo de software y hardware, Simulación y Capacitación.
- ✓ **Fase VII**: Año 2018. Centro de experimentación de Ciberdefensa y Capacitación.

El grupo de respuesta a emergencias cibernéticas de Colombia "COLCERT". Tendrá a su cargo, el desarrollo de tareas específicas, agrupadas así:

- ✓ **Infraestructura Crítica**:
  - Identificación del mapa de riesgos de la infraestructura crítica.
  - Diseñar e implementar una solución de monitoreo de infraestructura crítica
- ✓ **Asesoría a sectores económicos**:
  - Identificación de riesgos y diseño e implementación de estándares y protocolos (energía, TICs, financiero).
  - Creación de CSIRT's.
- ✓ **Cooperación Internacional**:
  - Adhesión al FIRST.
  - Creación del Centro de Excelencia
- ✓ **Política Pública**:
  - Política de Ciberseguridad y Ciberdefensa 2030.

VII. EFICIENCIA Y EFICACIA EN LA IMPLEMENTACIÓN DE LA GUIA DE CIBERSEGURIDAD.

Al implantar los lineamientos y políticas de "Ciberseguridad" y "Ciberdefensa", es esencial contemplar el seguimiento identificando el estado actual, con la finalidad de saber los resultados que se obtienen y si estos resultados cumplen los objetivos previstos.

Para ello hay que establecer procesos de auditoria, que permitan medir la eficacia y eficiencia de la implementación de la "GUÍA DE CIBERSEGURIDAD". Como instrumento para recoger de forma sistemática y representativa información relevante sobre el estado actual y los resultados de un proceso, plasmados en un informe, el cual está dedicado a emitir opiniones y el estableciendo de la eficiencia y eficacia sobre la situación de las operaciones auditadas.

Una auditoria puede clasificarse según quienes realizan el examen, siendo

auditorías internas cuando las personas que la practican forman parte del equipo auditor de la empresa auditada, se entiende por *auditoría externa* cuando el personal auditor no labora para la entidad auditada y es practicado por la contraloría o auditores independientes; una *auditoria gubernamental* es la que realizan expresamente auditores de la Contraloría general de la república, auditores internos del sector público y/o empresas privadas autorizadas por la contraloría general de la Nación para practicar este ejercicio en las empresas del estado.

Siguiendo la esencia neta del proceso de auditoría, esta es investigativa, analítica, critica y creativa en relación a los aspectos operacionales, administrativos, de la entidad auditada, sustentando su lógica en las matemáticas, estadísticas, comunicación, ética y en la teoría del conocimiento.

REFERENCIAS

[1]. CONSEJO NACIONAL DE OPERACIONES. GRUPO TECNOLOGICO. Guía De Ciberseguridad. BOGOTA D.C. C.N.O. 2011.

[2]. MINISTERIO DE MINAS Y ENERGIA. Sector Energía Eléctrica. Disponible en: http://www.minminas.gov.co/minminas/downloads/UserFiles/File/Memorias/Memorias_2011/05-ENERGIA.pdf

[3]. INFO SPYWARE. Latinoamérica dentro de los más afectados por la BotNet Mariposa. Disponible en: http://www.infospyware.com/blog/latinoamerica-dentro-de-los-mas-afectados-por-la-botnet-mariposa/

[4]. COMISION DE REGULACION DE TELECOMUNICACIONES. Recomendaciones Para La Creación De Una Estrategia Nacional De Ciberseguridad. BOGOTA D.C. CRT. Diciembre 13 de 2007.

[5]. MINISTERIO DE LAS TECNOLOGIAS Y LAS TELECOMUNICACIONES. Modelo De Seguridad De La Información Para La Estrategia De Gobierno En Línea. BOGOTA D.C. Octubre de 2011.

[6]. CONSEJO NACIONAL DE POLITICAS Y ECONOMIA SOCIAL. Lineamientos De Política Para Ciberseguridad Y Ciberdefensa. BOGOTA. CONPES. 2011.

[7]. MINISTERIO DE TECNOLOGIA DE LA INFORMACION Y LAS COMUNICACIONES. Lineamiento De Política Para La Ciberseguridad Y Ciberdefensa. COMPES 3701. Disponible en: http://www.mintic.gov.co/index.php/docs-normatividad?pid=698&sid=741:3701

[8]. MINISTERIO DE LA DEFENSA NACIONAL. Estrategia De Ciberseguridad Y Ciberdefensa. Bogotá D.C. Julio 14 de 2011.

[9]. García Vargas Juliana. Junio 2013. CIBERSEGUDIRAD Y CIBERDEFENSA EN COLOMBIA. Disponible en: http://www.oas.org/cyber/events/Colombia%20National%20Strategy.pdf