Propuesta para crear la unidad de seguridad cibernética nacional como ente superior gubernamental

Jesús Alberto Castro Mora
Diego Fernando Díaz Torres
Alexander Vásquez Ávila
Juan De Jesús Aquino De La Cruz
Cipriano Peña Chivatá

Trabajo de grado para optar al título profesional:
Especialización en Seguridad y Defensa Nacionales

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2016

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA

CEM 2016

PROPUESTA PARA CREAR LA UNIDAD DE SEGURIDAD CIBERNETICA NACIONAL COMO ENTE SUPERIOR GUBERNAMENTAL

MY. JESÚS ALBERTO CASTRO MORA CC. 9.272.187

MY. DIEGO FERNANDO DIAZ TORRES CC. 93.088.424

MY. VASQUEZ AVILA ALEXANDER CC. 93086731

MY. JUAN DE JESÚS AQUINO DE LA CRUZ CE. 585565

TUTOR

CR. (RA) CIPRIANO PEÑA CHIVATA

CEM 2016 "B"

TRABAJO DE GRADO ENTREGA FINAL

BOGOTÁ-COLOMBIA

2016

Tabla de contenido

Imágenes

PROPUESTA PARA CREAR LA UNIDAD DE SEGURIDAD CIBERNÉTICA NACIONAL COMO ENTE SUPERIOR GUBERNAMENTAL

Resumen

La manera en la cual Colombia está abordando el tema de seguridad cibernética es fundamental para presentar una iniciativa que contribuya a combatir amenazas de tipo cibernético, presentar un estudio sobre el estado de la seguridad cibernética, vulnerabilidades y fortalezas de Colombia , en búsqueda de proteger la infraestructura del estado colombiano por posibles amenazas de ataques cibernéticos, es por eso que ante estos riesgos el gobierno de Colombia creo la política nacional de seguridad cibernética *CONPES 3701* con el apoyo del ministerio de las tecnologías de la información y la comunicación TIC, el ministerio de defensa y otras instituciones públicas del estado las cuales constituyeron agencias de seguridad cibernética, entre ellas se creó el "*comando conjunto cibernético de las fuerzas militares*" (FFMM, 2012), lo importante para el país dentro de este proyecto de investigación, es que se establezca la unidad nacional de seguridad cibernética, con una política de cooperación internacional dirigida por una persona idónea en esta cultura organizacional nombrada por el gobierno nacional, en relación a que se instituya la normatividad correspondiente, con el fin de que el comando conjunto de ataques cibernéticos de las fuerzas militares adscrito al ministerio de defensa nacional, puedan trabajar mancomunadamente con las otras agencias de seguridad cibernética del estado, acorde con el objetivo de prevenir y mitigar los ataques informáticos, de la misma forma para garantizar el funcionamiento de sistemas de comunicación, navegación, información militar entre otros aspectos que pondrían en peligro el orden público en el país.

Palabras clave: *seguridad informática, seguridad cibernética, garantizar los sistemas de comunicación, cultura organizacional.*

PROPOSAL TO CREATE NATIONAL CYBER SECURITY UNIT AS TOP GOVERNMENT AGENCY

Abstract

The ministry of national defense and the ministry of technology and communication, to protect the infrastructure of the Colombian state for possible threats of cyber-attacks, so they created the "*command set of cyber-attacks by military forces*" (Armed Forces of Colombia , 2012), the important thing for the country within this research project is that the national unity of cyber security, led by a competent person in the organizational culture named in the national government regarding the establishment to which the regulations are instituted correspondingly, in order that the set of cyber-attacks from within the ministry of national defense military command, can work together with other agencies cybernetic security of the state, consistent with the objective of preventing and mitigating cyber-attacks, of the same way to ensure the operation of communication systems, navigation, military information among other things that would endanger public order in the country.

Keywords: *computer security, cyber security, secures communications systems, organizational culture.*

Introducción

"Hoy el hombre no vive ya en la naturaleza
Sino que está alojado en la sobre naturaleza
Que ha creado en un nuevo día
Del Génesis: la técnica."
(Ortega y Gasset).

Las fuerzas militares FFMM están ejerciendo sus operaciones de seguridad y defensa en todo el territorio nacional, actualmente hay otras clases de amenazas que pueden vulnerar el orden público, puesto que estamos viviendo en un mundo globalizado donde tiene gran dominio el internet, las redes sociales y la evolución tecnológica hacen que la teoría del profesor y filósofo canadiense Marshall Mc Luhan cobre mayor importancia sobre su postulado de la aldea global, y es así como se evidencia que esa comunidad virtual posee ciertos riesgos, los cuales pueden afectar la seguridad y defensa de esta aldea global a esto se le llama guerra ciberespacial, "*actualmente las guerras ya no se ganan en el campo de batalla tradicional, como fueron las trincheras; sino que ahora se obtienen en los medios de comunicación. En este sentido, es cada vez más el espacio simbólico que construyen los canales de comunicación y sus ampliaciones, donde se reconstruye y destruye los procesos de la vida cotidiana, particularmente en las ciudades"* (Madrid, 1997). Para contrarrestar este tipo de contingencias el ministerio de defensa nacional y la fuerza pública deben crear doctrina para prevenir y mitigar el riesgo de un ataque cibernético dentro de las escuelas de formación, pero la sola doctrina no ayudaría a atacar este flagelo, de ahí radica la importancia de establecer una política nacional en sistema de seguridad cibernética, dirigida por el gobierno nacional para que interactúen el "*comando conjunto cibernético de las fuerzas militares"* (FFMM, 2012), el centro cibernético policial y el equipo coordinador a nivel nacional de aspectos de seguridad informática, estas instituciones adscritas al ministerio de defensa conformarían el sistema nacional de seguridad cibernética con el fin de que establezcan planes de acción y matrices de riesgos para estar preparados y prevenir o mitigar estas nuevas amenazas.

En el capítulo uno se expondrá el origen de la seguridad cibernética, su historia de donde deriva la palabra cibernética, así mismo como se ha aplicado esta ciencia, desde que nacen las civilizaciones hasta la actualidad y como grandes pensadores entre ellos Norbert Wiener, y Niklas Luhmann generado grandes aportes al tema, de tal manera que hoy en día son tomados en cuenta cuando se habla de seguridad cibernética.

Según un estudio del banco interamericano de desarrollo BID y la organización de estados americanos *OEA "instan a América Latina y Caribe a mayores esfuerzos en ciberseguridad, dado que los últimos Informes sobre el tema demuestran que la región presenta vulnerabilidades "potencialmente devastadoras" Cuatro de cada cinco países carecen de estrategia de ciberseguridad*" (Observatorio de la Ciberseguridad , 2016) afirma este estudio que Colombia se encuentra en un nivel de madurez intermedio, pero que falta mucho para llegar a ser pioneros en materia de seguridad cibernética.

En el capítulo dos se expondrán los problemas que podría generar la creación de la unidad nacional de seguridad cibernética en el país en virtud de lo asegurado este proyecto de investigación propone construir una política de seguridad cibernética más acorde a las exigencias del mundo moderno y contemporáneo *Si vamos a sacarle la mayor ventaja posible a la llamada cuarta revolución industrial, tenemos que crear una infraestructura digital no sólo moderna y robusta sino también segura. Proteger a nuestros ciudadanos del cibercrimen no es una mera opción: es un elemento clave para nuestro desarrollo* (Observatorio de la Ciberseguridad , 2016).

En el capítulo tres se propone la estructura de la unidad nacional de seguridad cibernética, desafiando el reto que esto implica tanto para la sociedad como para las FFMM, en cumplimiento de su misión constitucional establecido en el capítulo 217 de la constitución política de Colombia de 1991, a fin de plantear una que surja de la cooperación entre los diversos actores el estudio pretende situar a américa latina en un nivel de madurez dinámico en materia de seguridad cibernética, Colombia está en un nivel intermedio de madurez, para lograr que sea más dinámico expondremos los aspectos relevantes de este estudio y como se puede mejorar el ámbito de seguridad cibernética en el país.

Finalmente se resalta en el último capítulo como se medirá la capacidad de preparación y formación del personal encargado de garantizar la optimización de la ciberseguridad con el fin de dar una potencial solución a la problemática expuesta, que ayude a mejorar la planeación estratégica de este fenómeno global. Para establecer los lineamientos solidos que contribuyan el fortalecimiento de la seguridad cibernética en Colombia, como una estrategia eficaz de solución a este flagelo una réplica puede ser que las fuerzas militares establecieran la creación de un centro de proyectos de investigación cibernética adscrito al comando conjunto de las fuerzas militares como intención de desarrollar proyectos en pro de la defensa ciberespacial.

Planteamiento del problema

En el mundo contemporáneo y globalizado el uso de las herramientas tecnológicas se ha convertido en una necesidad para el progreso y desarrollo de las naciones, ya que dichas herramientas permiten que se agilicen procesos y trasporte información en tiempo record, esto puede visualizarse como una fortaleza si se le da un manejo adecuado, pero irónicamente también puede convertirse en una eventual riesgo para la seguridad de un país, dado a la magnitud de la información que se puede manejar mediante la cibernética, y de ser irrumpida se consolidaría en un riesgo nacional, tomando esto como punto de partida se puede ahondar en las teorías planteadas por el profesor y filósofo canadiense Marshall Mc Luhan acerca de la importancia de la aldea global, y es así como se evidencia que esa comunidad virtual posee grandes riesgos, los cuales pueden afectar la seguridad y defensa de una nación, a esto se le llama guerra ciberespacial, para contrarrestar este tipo de contingencias es necesario establecer una política nacional direccionada a garantizar el sistema de seguridad cibernética en el país, y la cual estaría coordinada por el gobierno nacional a fin de que se pueda existir una interacción con todas las agencias del estado relacionadas en aspectos de seguridad informática, estas instituciones adscritas al ministerio de defensa conformarían la unidad nacional de seguridad cibernética con el fin de que establezcan planes de acción y matrices de riesgos para estar preparados y prevenir o mitigar este conflicto global.

¿Cómo se puede establecer la unidad de seguridad cibernética nacional en aras de proteger las infraestructuras críticas de la información en el país?

Antecedentes

Con el fin de realizar un estudio detallado de las referencias que acontecen, del por qué se implementó un sistema de seguridad cibernética a nivel mundial, en el 2007 del mes de abril se dio origen a uno de los eventos más famosos en materia de ataques cibernéticos, en Estonia, producto de una decisión política del gobierno local de trasladar los cuerpos de soldados soviéticos muertos y un monumento del soldado de bronce, un emblema de la ocupación militar soviética perpetrada durante la segunda guerra mundial, hacia un cementerio militar, el gobierno ruso tuvo fuertes tensiones respecto al tema y manifestó que mencionados hechos son un profanación inhumana, Rusia amenazo con sanciones económicas, sociales, y políticas a su país vecino.

Con todos estos hechos se da un evidente deterioro en las relaciones diplomáticas entre Rusia y Estonia lo cual generaron múltiples protestas entre los nacionalistas rusos en Estonia, surgieron ataques cibernéticos por parte de Rusia, estos ataques estaban direccionados a bloquear todo tipo de servicios de internet lo que conllevo |a una desorganización para todo el país debido a su gran sometimiento y dependencia al Internet, dichos ataques hicieron que las páginas no se abran comúnmente y en el instante producto de una sobrecarga del sistema, generando problemas para utilizar los bancos, medios de comunicación y otra clase de servicios los cuales dependían de una red móvil esto fue durante un lapso de tres semanas, *Rusia fue considerada la principal responsable por los ataques cibernéticos de Estonia, pero rechazó la atribución. Considerando este escenario caótico, en este artículo se busca investigar la prevención de la guerra cibernética, más precisamente la disuasión cibernética. Para eso, en la primera parte se investiga el concepto de guerra cibernética y en la segunda parte, el concepto de disuasión cibernética, esto demando la intervención de la comunidad internacional* (sandroni, 2010), los cuales pusieron en su agenda la preocupación por los ataques cibernéticos y crearon centros de cooperación de ciberdefensa para que los países miembros de estas comunidades internacionales, estuvieran prevenidos y tuvieran el experticia pertinente para actuar ante una amenaza cibernética.

En el 2008 los ataques informáticos no cesaron, los hackers crearon un virus llamado conficker que infecto a más de 12 millones de ordenadores del reino unido vulnerando los sistemas de navegación de la armada y del parlamento de ese país.

En el 2009 Ciberdelincuentes lograron vulnerar el sistema informático del pentágono y hurtaron información muy valiosa como las características tácticas y técnicas de un avión caza del ejército de Estados Unidos el F-35, según las agencias de seguridad esta información puede ser utilizada por muchos países para crear mecanismos de defensa contra este tipo de aeronaves.

El 22 de mayo del 2012 se tuvo conocimiento que Anonymous una sociedad de personas indignadas contra las instituciones públicas de los estados, emplean sus protestas con ataques cibernéticos, vulnerando así los sistemas de seguridad de la información del Ministerio de Justicia de EEUU, de tal manera que se pudo acceder fácilmente a la información de datos contra la vida de las personas y cometer toda clase de delitos cometidos en este país.

Estos son los casos más famosos de ataques cibernéticos, con estas lecciones aprendidas es donde los países implementaron grupos de respuesta ante estas amenazas, en el caso colombiano nuestro sistema de seguridad cibernética se encuentra en un nivel formativo lo que requiere de mucho trabajo dentro de las cinco de dimensiones para llegar a un nivel de madurez dinámico que permita contrarrestar todo tipo de amenazas a la seguridad de la información.

Algunos términos clave dentro del espectro de seguridad cibernética Glosario y definición

Antivirus: es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles (Symantec., 2016).

Las aplicaciones engañosas: son programas que intentan engañar a los usuarios informáticos para que emprendan nuevas acciones que normalmente están encaminadas a causar la descarga de malware adicional o para que los usuarios divulguen información

personal confidencial. Un ejemplo es el software de seguridad fraudulento, que también se denomina scareware (Symantec., 2016).

Ataque Web: es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta (Advisory Services, 2015).

Botnet: Conjunto de equipos bajo el control de un bot maestro, a través de un canal de mando y control. Estos equipos normalmente se distribuyen a través de Internet y se utilizan para actividades malintencionadas, como el envío de spam y ataques distribuidos de negación de servicio. Las botnet se crean al infectar las computadoras con malware, lo cual da al atacante acceso a las máquinas. Los propietarios de computadoras infectadas generalmente ignoran que su máquina forma parte de una botnet, a menos que tengan software de seguridad que les informe acerca de la infección (Rojas, 2012).

Caballo de Troya: código malicioso el cual aparenta ser algo que no es. Los caballos de troya tienen códigos maliciosos que cuando se activan causa pérdida, incluso robo de datos. Por lo general, también tienen un componente de puerta trasera, que le permite al atacante descargar amenazas adicionales en un equipo infectado.

Canal de mando y control: es el medio por el cual un atacante se comunica y controla los equipos infectados con malware, lo que conforma un botnet (Rojas, 2012).

Crimeware: Software que realiza acciones ilegales no previstas por un usuario que ejecuta el software. Estas acciones buscan producir beneficios económicos al distribuidor del software (Symantec., 2016).

Ciberdelito: es un delito que se comete usando una computadora, red o hardware. La computadora o dispositivo puede ser el agente, el facilitador o el objeto del delito. El delito puede ocurrir en la computadora o en otros lugares.

Ciberamenaza: advertencia de daño a los sistemas y servicios presentes en el ciberespacio (Symantec., 2016).

Ciberarma: programa o dispositivo diseñado para realizar ciberataques (Symantec., 2016).

Ciberataque: manejo del ciberespacio para atacar a los sistemas y servicios plataformas tecnológicas entre otros; acceder sin autorización a información, o alterar o impedir el funcionamiento de los servicios o programas (Symantec., 2016).

Ciberespacio: Espacio virtual mundial que interconecta sistemas de información, dispositivos móviles y sistemas de control industrial. Está soportado por todo tipo de comunicaciones tales como internet y redes de telefonía móvil. La interconexión proporciona acceso en línea a información y servicios.

Ciberoperaciones: Operaciones militares conducidas en el ciberespacio (Symantec., 2016).

Ciberseguridad: Conjunto de actuaciones orientadas a hacer más seguras las redes y sistemas de información que constituyen el ciberespacio; detectando y enfrentándose a intrusiones; detectando, reaccionando y recuperándose de incidentes; y preservando la confidencialidad, disponibilidad e integridad de la información (Symantec., 2016).

Ciberguerra: El uso de capacidades basadas en la red de un estado, para interrumpir, denegar, degradar, manipular o destruir información residente en ordenadores y redes de ordenadores, o los propios ordenadores y las redes de otro estado (Symantec., 2016).

Capitulo Uno; Origen de la seguridad cibernética y su proyección en Colombia mediante un estudio prospectivo

En este capítulo se expondrá el origen de la seguridad cibernética, de donde deriva la palabra cibernética, así mismo como se ha aplicado esta ciencia, desde que nacen las civilizaciones hasta la actualidad y como fundamentados en teorías expuestas por grandes pensadores y filosos entre ellos Norbert Wiener, y Niklas Luhmann sustentan un tema tan controversial como es el de la seguridad cibernética.

Pese a que la cibernética es catalogada como un tema contemporáneo, este surge de la necesidad de optimizar procesos que mejorarían el niel de la vida de la humanidad, en el caso específico de Colombia cabe destacar la importancia de una proyección prospectiva para enfocar los esfuerzos gubernamentales con el fin de ser pioneros en esta materia, y así contribuir con desarrollo sustentable en una sociedad política.

Los conceptos o tecnicismo cibernéticos son nuevos y esporádicos, pero tienen una relación estrecha con el interés del mejoramiento de las condiciones de vida de las personas, permitiendo que la información se traslade en menor tiempo posible y ofreciendo herramientas que fortalecen la comunicación entre los seres humanos, y de alguna manera se ajusta a las premisas de Aristóteles filosofo de origen griego quien a planteó la teoría de la "sociabilidad natural", donde se sincretiza al hombre como un animal social que necesita de otros para poder sobrevivir, es por eso desde esos tiempos se pensaba en cómo crear una sociedad en la que todos pudieran vivir en comunidad, desempeñando unos roles afines a su calidad social, siempre evocando entre todo el bien común y la ética como guía principal de la vida.

Historia de la Cibernética

La palabra cibernética se deriva del griego (kybernetes) el cual significa *"arte de manejar un navío", o arte de un timonel o pilotear*, (Rojas, 2012) los griegos mencionaron kybernetes, al gobierno de la nave, que realizaba el timonel del barco, un ejemplo claro de aplicación de esta palabra fue dentro de las grandes fiestas atenienses se hacían homenajes a las "Cibernesias" o fiesta de los pilotos. Es importante manifestar que fueron los griegos los

que sacaron de contexto la palabra Kybernetes en el área o campo de los navíos, para introducirla en el arte de gobernar fue Platón con su obra la república, donde kybernetes fue más acuñado al arte de dirigir o gobernar a los hombres.

La palabra cibernética la introdujo a la comunidad científica después de mucho tiempo Norbert Wiener, fue un matemático estadounidense, conocido como el padre de la de la cibernética mediante su obra *Cibernética o el control y comunicación en animales y máquinas* (Rojas, 2012), publicado en 1948, es por eso que a nivel mundial se le otorga a Norbert Wiener haber utilizado por primera vez este concepto en una de sus publicaciones, el término "Cibernética" lo definía de una manera pragmática *"como el estudio interdisciplinario de la estructura de los sistemas reguladores y de información"* (cruz, 2012). Su obra sobre cibernética actualmente sirve como apoyo y baluarte en todas las universidades y centros de formación donde capacitan, todo lo acontecido con seguridad y defensa cibernética (Solorio, 2011). Este es un término genérico y antiguo pero aún usado para muchas áreas que están incrementando su enfoque cuantitativo en áreas como, hacker, teoría de información, programación, Ingeniería de Sistemas, seguridad informática encriptación entre otras ciencias de la información.

Es el estudio de sistemas abiertos en cuanto a la energía y cerrados en cuanto a la información y al control. Asimismo Wiener redefinió a la cibernética como al estudio analítico del isomorfismo de la estructura de las comunicaciones en los organismos y en las sociedades, entendiéndose por isomorfismo una identidad entre dos sistemas, que para que exista se requiere de determinadas relaciones entre los objetos del otro (Vasco, 2008).

Dentro de sus postulados Wiener concibió *que, de nuestras sociedades, es imposible conseguir los objetivos principales de la vida en común sin la información necesaria en el momento y lugar precisos* (Vasco, 2008). Este filosofo matemático, sociólogo ingeniero y físico elaboro un sin número de estudios de lógica matemática llegando a probar de manera irrefutable cómo fracasarían nuestras sociedades si la información, la cual es fundamental no es entregada a la gente indicada en el momento oportuno. Sin lugar a dudas Wiener subrayó siempre la condición de comunicador del ser humano; condición que lo diferenciaba de otros seres.

Otro de los grandes precursores de la cibernética es Niklas Luhmann manifestando que *la sociedad moderna es un sistema Constituido, no tanto por individuos sino por comunicación, se diferencia en subsistemas funcionales cerrados a través de códigos especializados: los sistemas político, económico, religioso, artístico jurídico* (Vasco, 2008).Este importante visionario desde ya dejo ver que era uno de los más relevantes pensadores alemanes sus postulados se agrupan en la elaboración de una teoría de la sociedad, describiendo a la sociedad misma como un sistema el cual de la misma forma sea el eje central de las comunicaciones.

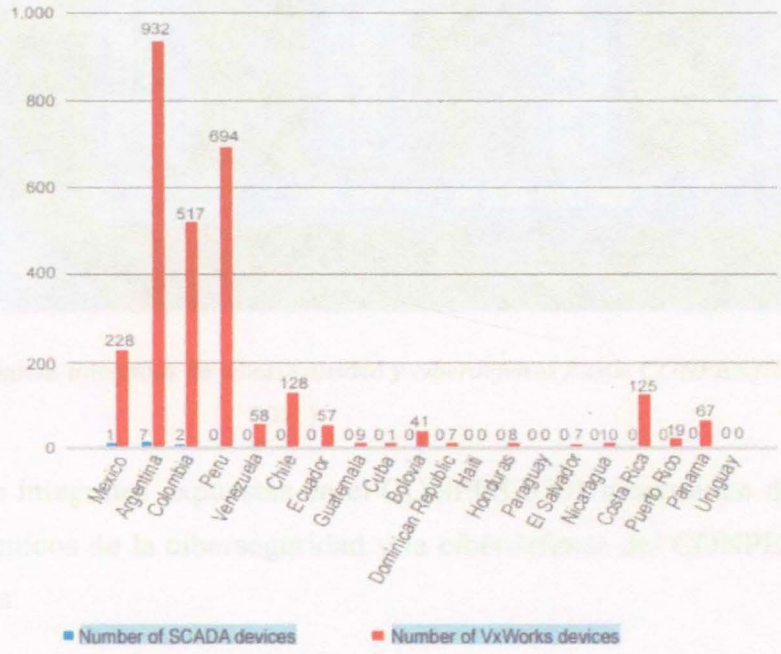
El legado de Luhmann concentra componentes muy novedosos, para la época procedentes de la cibernética, Luhmann proporciona un instrumento que permita realizar observaciones y herramientas solidad con el propósito de controlar la sociedad contemporánea, mediante un diagnostico que pretenda diseñar nuevas estrategias para actuar sobre ella. Su obra expone diseñar nuevas formas de pensamiento que sean capaces de abordar las exigencias de nuestro tiempo dentro del marco de un mundo altamente globalizado

La seguridad cibernética en Colombia

Las amenazas cibernéticas expuestas en los antecedentes de este proyecto de investigación han determinado la importancia de mantenerse actualizado en afinidad a las novedades, las cuales se encuentran en torno a la delincuencia cibernética, hacer énfasis en las políticas de seguridad integral cibernética fue la iniciativa del actual gobierno para destinar un rubro financiero dentro del presupuesto público para crear un grupo de respuesta a emergencias cibernéticas y demás agencias de ciberdefensa del estado, así las cosas en la actualidad se encuentran en un nivel de madurez formativo y establecido, para llegar a un nivel dinámico se requieren de muchos esfuerzos lo importante es estar en el camino del éxito hacia una política que aporte a generar soluciones a los eventuales riesgo que se puedan presentar.

Mediante un estudio elaborado en Colombia ha tenido un sin número de ataques informáticos la página de la presidencia de la República, ha sido vulnerada Gobierno y el ministerio de defensa nacional entre otras instituciones públicas del estado dejaron fuera de servicio varias páginas la modalidad introducir códigos maliciosos otro de los casos

emblemáticos de Ciberamenazas en Colombia son *casos como robo de identidad, robo a cuentas bancarias que a 2009 llegaban a 50.000.000 millones del mismo modo intento atentarse contra la infraestructura crítica de la nación, pero estos fueron repelidos. Sin embargo, los organismos de seguridad colombianos son conscientes del hecho que el nivel de sofisticación de los ataques va en aumento y es necesario tener en cuenta ello para evitar problemas en el futuro* (Rojas, 2012). El que lleva la dirección en el país de la ciberseguridad y ciberdefensa es el ministerio de defensa nacional aunque COLCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia) el cual trabaja en conjunto con el ministerio de las tecnologías de la información y la comunicación, el ministerio del interior y el ministerio de la cultura.

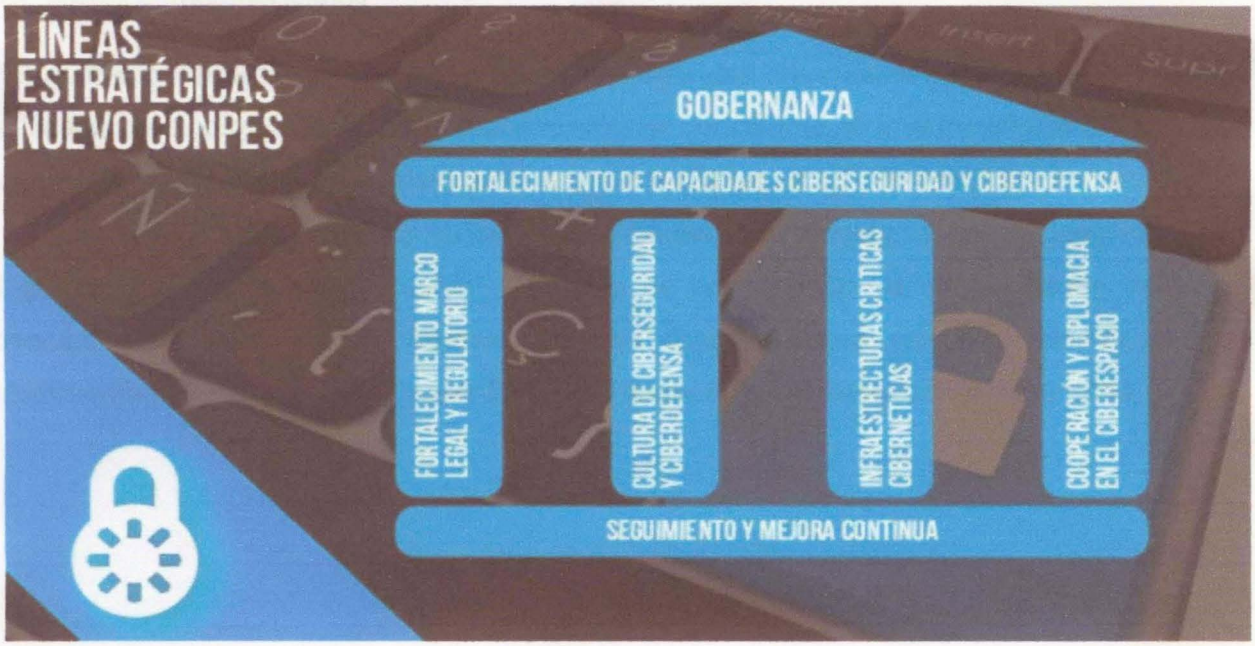


Number of Internet-Facing SCADA and VxWorks Devices in the Americas and the Caribbean
Fuente: http://www.shodanhq.com/

Imágenes 1número de dispositivos infectados por "scada" supervisión y control de datos y número de dispositivos infectados por un sistema operativo vxworks (Rojas, 2012)

En la gráfica No 1, se videncia mediante un diagrama "vxworks" los potenciales riesgos en un ordenador, la barra roja representa el número de dispositivos infectados por un sistema operativo de datos que se puede encontrar en cualquier ordenador o CPU y la barra azul muestra una barra azul "Scada" los datos que han sido vulnerados por un software o programa

que permite controlar y supervisar procesos de forma industrial, Colombia en el año del 2012 registro 517 ataques cibernéticos contra sistemas operativos, caseros o empresariales los cuales utilizaban un "host "este término quiere decir computadoras conectadas a una red (Observatorio de la Ciberseguridad , 2016).



Imágenes 2 Líneas estratégicas integrales de ciberseguridad *y ciberdefensa fuente CONPES3701* (Social, 2011)

Las líneas estratégicas integrales expuestas en el CONPES 3701 determinan de manera detallada los aspectos técnicos de la ciberseguridad y la ciberdefensa del CONPES están a cargo de tres instituciones:

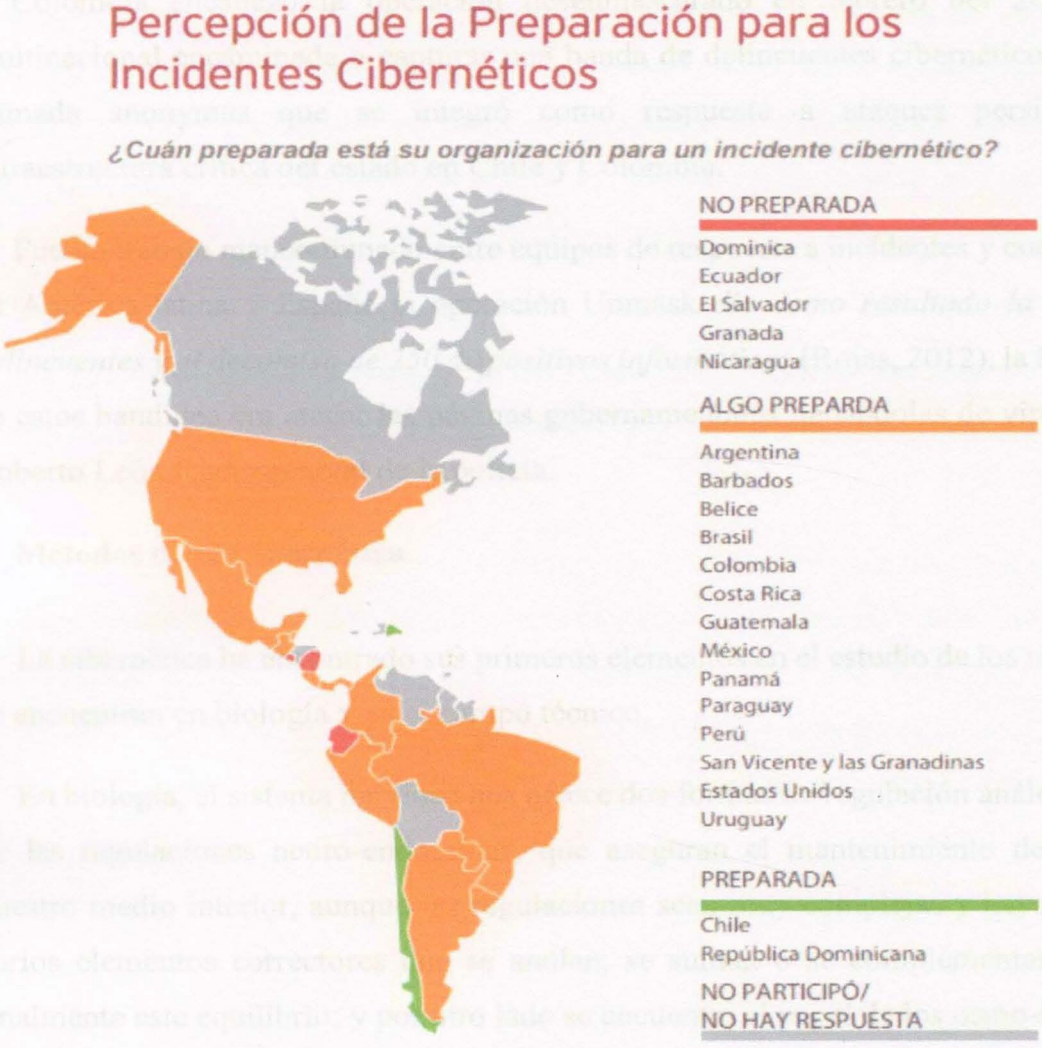
El Centro Cibernético Policial (CCP), responsable de asegurar la integridad de las redes policiales y de la sociedad civil y que mantiene una vigorosa capacidad de investigación (Social, 2011).

El Comando Conjunto Cibernético (CCOC), una unidad militar que responde a ataques contra los bienes militares de la nación (Social, 2011).

El colCERT la entidad coordinadora a nivel nacional que supervisa todos los aspectos de la ciberseguridad y la ciberdefensa (Social, 2011).

COLCERT en 2012 Contribuyó a la captura en Colombia, de un delincuente cibernético llamado Jorge Maximiliano Pachón alias el zar de la clonación, pacho como se le conocía en el mundo delincuencial, fue arrestado con *más de 8.000 tarjetas de crédito clonadas a la mano y tras amasar más de US$9 millones* (Rojas, 2012). Sus delitos cibernéticos estaban en cinco países latinoamericanos

El gobierno colombiano con las agencias de seguridad cibernética consiguió determinar que los usuarios colombianos tienen *bajos niveles de conciencia de la seguridad cibernética, lo que precipitaba hábitos de navegación inseguros* (Rojas, 2012), lo cual hace los usuarios de internet más vulnerables a ser víctimas de estos delitos. Además, la escasa capacitación del gobierno nacional sobre ataques y la falta de cooperación o comunicación de los proveedores de servicios de internet y otras organizaciones privadas constituyeron impedimentos importantes para poner freno a la delincuencia cibernética en Colombia.



Imágenes 3. Percepción de la preparación para los incidentes cibernéticos fuente tomada por Mc CAFFE

En la gráfica No 3 se puede observar como el sistema de seguridad cibernética colombiano esta algo preparado para cualquier tipo de incidentes, así mismo muestra a América latina y el Caribe, en el tema de ciberseguridad que carece de mayor efectividad a la hora de enfrentar una amenaza cibernética, el único país que se salva a este tipo de inconvenientes globales es chile.

Operación "unmask" desenmascarado Colombia

Colombia encabezó la operación desenmascarado en febrero del 2012, una tarea multinacional encaminada a capturar una banda de delincuentes cibernéticos internacional llamada anonymus que se integró como respuesta a ataques persistentes contra infraestructura crítica del estado en Chile y Colombia.

Fue un trabajo mancomunado entre equipos de respuesta a incidentes y cuerpos policiales de América latina y España la operación Unmask *dio como resultado la captura de 25 delincuentes y al decomiso de 250 dispositivos informáticos* (Rojas, 2012), la forma de operar de estos bandidos era atacar las páginas gubernamentales llenándolas de virus explicó José Roberto León Riaño general de la policía.

Métodos de la Cibernética

La cibernética ha encontrado sus primeros elementos en el estudio de los reguladores, que se encuentran en biología y en el campo técnico.

En biología, el sistema nervioso nos ofrece dos formas de regulación análogas. Es el caso de las regulaciones neuro-endocrinas, que aseguran el mantenimiento del equilibrio en nuestro medio interior, aunque las regulaciones sean muy complejas y hayan de intervenir varios elementos correctores que se anulan, se suman o se complementan, para realizar finalmente este equilibrio; y por otro lado se encuentra el papel de los osmo-receptores en el control de la concentración osmótica del plasma; en este caso la hormona antidiurética desempeña un papel intermedio para regular la eliminación renal de agua.

La analogía es más sorprendente cuando se examinan los problemas musculares. El estar de pie, por ejemplo, se posibilita mediante el juego de los músculos de la estática que, por una serie de contracciones y dilataciones, aseguran el equilibrio del conjunto.

La flexión de una pata posterior engendra una serie de contracciones y relajaciones rítmicas, en tanto dura la flexión. Asistimos al fenómeno del "clonus", bien conocido en neuropatología, en los síndromes piramidales. N.Wiener, considerado como el padre de la

cibernética, ha estudiado matemáticamente el fenómeno de clonus y ha podido establecer relaciones entre la experimentación y él calcula.

Existen otras analogías, como los circuitos reverberantes u oscilantes que se encuentran en electrónica; algunos han conocido un determinado favor, como el esquema construido por Bucy para tratar de explicar la teoría de los movimientos involuntarios. La careoatetosis con sus movimientos desordenados y el mal de Parkinson con su temblor asociado a la parálisis, parecen responder a la existencia de circuitos oscilantes entre la corteza cerebral y los núcleos de la base del cerebro.

Las calculadoras electrónicas y las máquinas de traducir no son más que el embrión de una actividad cerebral supuesta, cuyo trabajo no corresponde probablemente a lo que pasa realmente en los circuitos nerviosos.

Esta conclusión por pesimista que sea, no rebate sin embargo a los cibernéticos, cuyo fin no es revolucionar el mundo con los "robots", sino simplemente buscar mejor la forma de comprender el funcionamiento de los organismos vivientes con ayuda de analogías mecánicas o eléctricas. Estas analogías no existen sino que a veces es necesario crearlas; esto es lo que ha dado lugar a los animales sintéticos (como tortugas, ranas etc.).

Capitulo Dos; Las Amenazas Y Vulnerabilidades De La Unidad De Seguridad Cibernética Colombiana

En este capítulo se expondrán los problemas que podría generar la creación de la unidad nacional de seguridad cibernética en el país, puesto que este proyecto estratégico tendría que ver con el presupuesto público, y vale resaltar que actualmente todos los esfuerzos del gobierno nacional están orientados hacia la construcción de una paz estable y duradera "En la discusión del Presupuesto General de la Nación para 2016 se aforan 215,9 billones de pesos, direccionados en una eventual etapa de posconflicto" (El Espectador , 2015) donde hay que resarcir a las víctimas del conflicto armado interno, los que resulta preocupante puesto que se dificulta la asignación de recursos para la creación de la Unidad de seguridad cibernética "*El Gobierno nacional destinará el año próximo unos 10 billones de pesos para el postconflicto que puede llegar si se firma la paz con las FARC, que se calcula requerirá una inversión de 90 billones de pesos en la próxima década*" (Heraldo, 2015). Así mismo otro factor que podría obstaculizar la inversión en la creación del sistema nacional de seguridad cibernética es el plan del gobierno por mejorar la infraestructura vial con la construcción de concesiones viales de cuarta generación, "*Colombia ha iniciado un ambicioso plan de desarrollo de infraestructura vial que requiere de altos montos de inversión. Estamos firmemente comprometidos en contribuir a acelerar el financiamiento de estos grandes proyectos de infraestructura, que sin duda contribuyen al desarrollo del país, mejorando su competitividad a nivel regional", dijo Andrés Castro, presidente de Sura Asset Management para Latinoamérica, holding de inversión del Grupo Sura*" (Espectador, 2016). Es el tema del posconflicto resulta ser un gran inconveniente puesto que la asignación presupuestal para resocialización de los grupos ilegales alzados en armas debe ser incrementada de manera considerable, oponiéndose indirectamente a la creación de un sistema nacional de seguridad cibernética, puesto que para consolidar dicha iniciativa se debe contar un presupuesto que permita validar todos los recursos, así mismo este tema debe incluirse en las políticas planteadas por el gobierno.

Con base a un estudio elaborado por el banco interamericano de desarrollo y la organización de los estados americanos falta de fundamentos e infraestructura educativa en seguridad cibernética no existen especializaciones profundas en este tema específicamente,

las leyes como medidas pasivas y el procedimiento penal de delincuencia cibernética están bien desarrollados en Colombia. Se deben optimizar las capacidades y destrezas que permitan destacar las habilidades cibernéticas en la aplicación de la ley, como se indica en los datos proporcionados por los países de América Latina y el Caribe en diversos estudios, Colombia en el marco legal de la seguridad cibernética se encuentra en etapa formativa mediante la cual ha aprobado una legislación procesal penal integral y de efectiva penalización (Ley 1273 y Ley 906) para condenar los delitos cibernéticos y reconoce los tratados internacionales con Interpol y Europol, así como las fuerzas del orden y el Poder Judicial.

El crecimiento del uso de internet en Colombia ha subido inconmensurablemente el número de usuarios cada día es mayor, sin embargo las falencias son en capacitación y el manejo de la información hábitos que hoy en día los cibernautas colombianos en su mayoría no tienen un conocimiento idóneo para afrontar todo tipo de ataques.

Figura 1. Crecimiento del uso de Internet Colombia 2000-2009

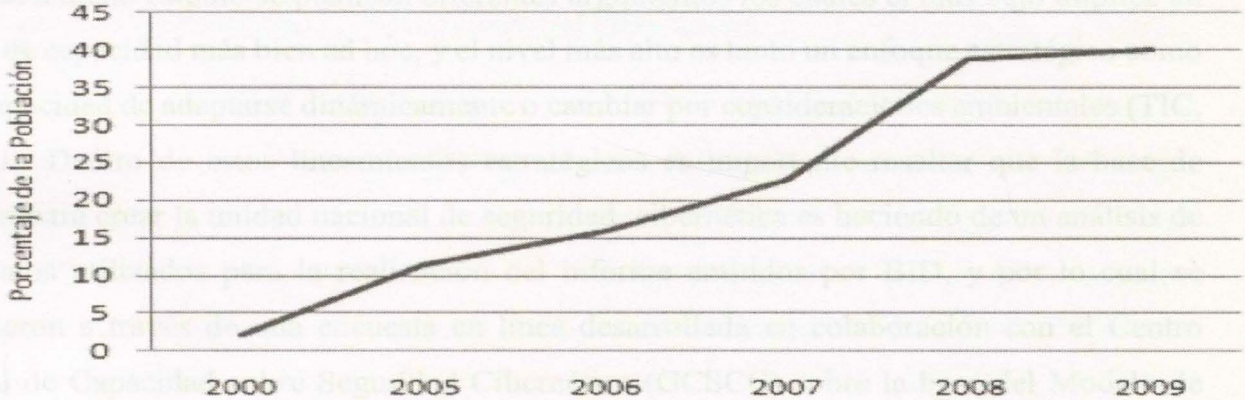


Figura 1 Crecimiento del uso de Internet Colombia 2000-2009

Fuente: Ministerio de Defensa Nacional de Colombia

Imágenes 4. Crecimiento del uso de internet en Colombia fuente tomada por: (Rojas, 2012)

La imagen cuatro muestra el incremento de usuarios de internet en Colombia desde el año 2000 hasta el año 2009 el porcentaje de la población muestra que en el 2009 ya había un acceso al internet del 45% de la población colombiana, en la actualidad en el año 2016

muestra un crecimiento del 80% lo que quiere decir que 8 de cada 10 colombianos tienen acceso optimo al internet, este dato es relevante si se considera que desde el 2009, los colombianos pasan más tiempo en sus ordenadores, esto incrementa la necesidad de los productores y fabricantes no solo de hardware sino también de software amplíen sus mercados y ofrezcas nuevas aplicaciones, las cuales si se les da un manejo inadecuado pueden llegar a extralimitar en sus funciones.

Capacidad y nivel de madurez de la seguridad cibernética en Colombia

El tema de la ciberseguridad has sido tratado por diferentes sectores económicos del mundo, y como resultado de uno de los estudios hecho por el banco interamericano de desarrollo BID y de la organización de los estados americanos OEA, mediante el observatorio de la seguridad cibernética para América latina puso en conocimiento el *"grado de madurez"* de la Ciberseguridad en Colombia, para eso exponen los cinco aspectos de niveles de madurez con los que puede medir la capacidad de seguridad cibernética en Colombia, de acuerdo a dicho estudio se plantean diferentes argumentos los cuales el más bajo implica un grado de capacidad más bien ad hoc, y el nivel más alto es tanto un enfoque estratégico como una capacidad de adaptarse dinámicamente o cambiar por consideraciones ambientales (TIC, 2012)*).* Dentro de estos lineamientos estratégicos es importante resaltar que la base de estudio para crear la unidad nacional de seguridad cibernética es haciendo de un análisis de Los datos utilizados para la realización del informe emitidos por BID, y por lo cual se recogieron a través de una encuesta en línea desarrollada en colaboración con el Centro Global de Capacidad sobre Seguridad Cibernética (GCSCC) sobre la base del Modelo de Madurez de Capacidad de Seguridad Cibernética (CMM, por sus siglas en inglés) desarrollado por el GCSCC (Observatorio de la Ciberseguridad , 2016).

A los estados miembros del observatorio de la ciberseguridad para América latina y el Caribe se elaboró un análisis detallado de la seguridad cibernética y del perfil de seguridad, con el propósito de proyectar mediante un análisis prospectivo mejores condiciones de seguridad y ser pioneros dentro del ámbito de seguridad cibernética. Según el Modelo de Madurez de Capacidad de Seguridad Cibernética estos niveles de madurez se dividen en 5 dimensiones:

1) Políticas y estrategia nacional de seguridad cibernética ("Políticas y estrategia");

2) Cultura cibernética y sociedad ("Cultura y sociedad");

3) Educación, formación y competencias en seguridad cibernética ("Educación");

4) Marco jurídico y reglamentario ("Marco jurídico");

5) Normas, organizaciones y tecnologías ("Tecnologías"). (Observatorio de la Ciberseguridad , 2016)

Cada dimensión posee componentes los cuales ayudan a un estado más maduro de capacidad en materia de seguridad cibernética (diario, 2016).Y tienen unos niveles importantes para indicar el estado de madurez. Esto ayudara a Colombia a mejorar el nivel máximo para crear un sistema más dinámico, más adaptable, más riguroso de acuerdo a los postulados hechos por el observatorio de seguridad cibernética para América latina y el Caribe.

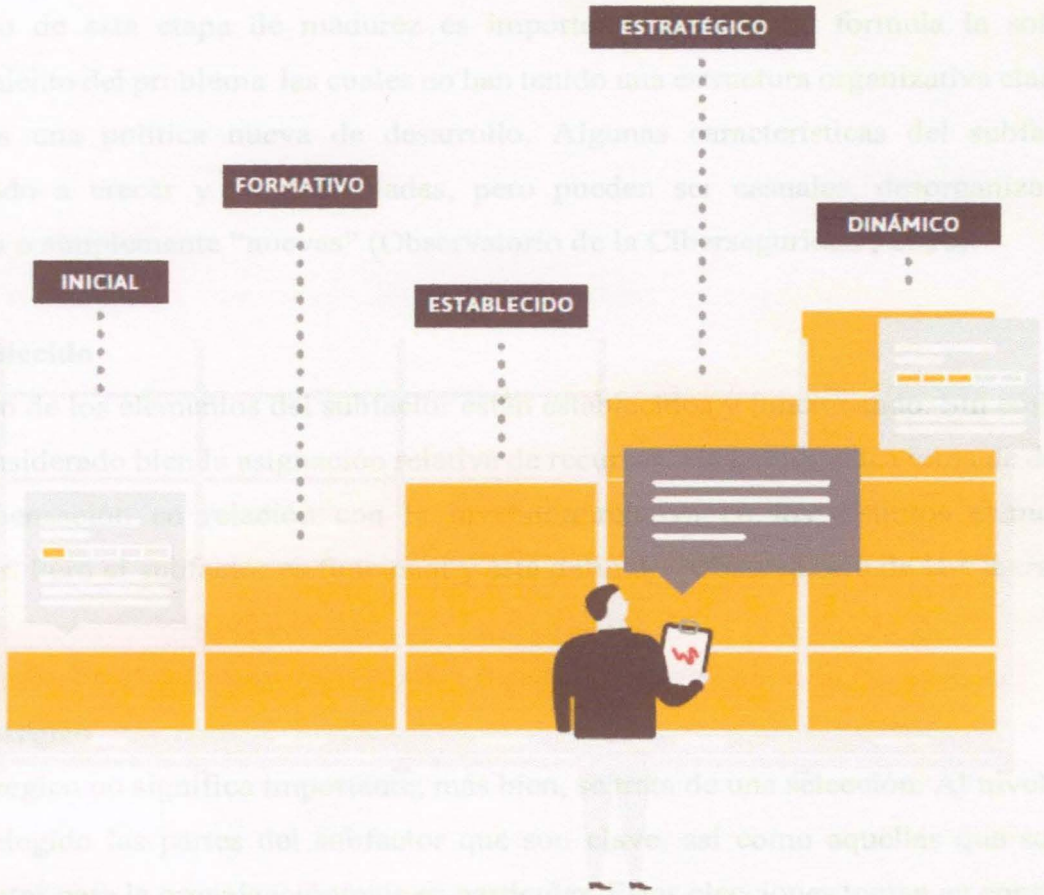
Los cinco niveles de madurez de la seguridad cibernética

Según los expertos en el tema, la mayor parte de las organizaciones del país, no están lo suficientemente capacitados, evento en el cual no son competentes para disminuir los riesgos informáticos que deben enfrentarse en la actualidad, esta premisa se fundamenta en que cuando se desarrollan actividades académicas y de capacitación en el tema de ciberseguridad, su enfoque no está alineado a la amenaza de la plataforma actúa, puesto que a Colombia los avances tecnológicos tardan en llegar (Observatorio de la Ciberseguridad , 2016). La madurez en tema de seguridad cibernética en Colombia es de nivel medio, lo que resulta sorprendente, ya que muchas organizaciones encuestadas por el observatorio de ciberseguridad para América latina y del Caribe reportaron incidentes de seguridad que dieron lugar a la pérdida o daño de sus procedimientos.

La mayor capacidad de los sistemas de ciberseguridad está enfocada generalmente en lo relacionado a producción, esto resalta que la verdadera falencia en el tema es crear mecanismos los cuales ayuden a descubrir las posibles amenazas cibernéticas y prevengan todo tipo de riesgos en el tema.

Esto explica el nivel intermedio de madurez en materia de ciberseguridad de Colombia, dejando en evidencia la necesidad de plantear estrategias de seguridad en temas cibernéticos, pero aún sigue estando lejos de países avanzados en el tema como lo son Estados Unidos, Israel, Estonia o República de Corea, así lo explicó un informe que fue publicado por el Banco Interamericano de Desarrollo (BID) y la Organización de Estados Americanos (OEA). Esto quiere decir que los cimientos de seguridad cibernética apenas están comenzando, y falta mucho por hacer, para iniciar el proceso de fortalecimiento de fortalecimiento es importante definir la estrategia que será solida con el fin de que en Colombia se centralice la información mediante la creación de la unidad nacional de seguridad cibernética "el estudio del banco interamericano de desarrollo deja ver que dos de cada tres naciones de la región no cuentan con un centro de comando y control de seguridad cibernética (diario, 2016)" lo que disminuye la capacidad de respuesta a incidentes cibernéticos de los países de América latina y el Caribe, como una fase inicial de las consolidación de la unidad cibernética se deben establecer mecanismo que ordenen y controlen las maniobras planteadas en marco de legalidad, puesto que a la fecha no hay componentes óptimos de mando y observación también este estudio nos permite ver que solo seis naciones cuentan con un programa estructurado de educación en seguridad cibernética.

Hace falta más dinamismo entorno a la seguridad cibernética, Israel es pionera en esta materia, es importante recalcar si un centro de proyectos e investigaciones en seguridad cibernética podría estudiar las tendencias y el dinamismo con el que cuenta la seguridad cibernética israelí para así mismo aplicar estas iniciativas vanguardistas en Colombia.



Imágenes 5; niveles de madurez de la seguridad cibernética fuente tomada por el observatorio de la seguridad cibernética para América latina y el caribe (Observatorio de la Ciberseguridad , 2016)

Niveles de madurez en aspectos cibernéticos.

Inicial

En síntesis incluye un pensamiento o una observación acerca de un problema (Observatorio de la Ciberseguridad , 2016), pero no una acción. Se encuentra en una fase primitiva donde solo es parte o tema de discusión en algunos sectores de educación o un interés de algún funcionario público.

Formativo

Dentro de esta etapa de madurez es importante afirmar, se formula la solución al planteamiento del problema las cuales no han tenido una estructura organizativa clara debido a que es una política nueva de desarrollo, Algunas características del subfactor han comenzado a crecer y ser formuladas, pero pueden ser casuales, desorganizadas, mal definidas o simplemente "nuevas" (Observatorio de la Ciberseguridad , 2016).

Establecido

Dentro de los elementos del subfactor están establecidos y funcionando. Sin embargo, no se ha considerado bien la asignación relativa de recursos. Ha habido poca toma de decisiones de compensación en relación con la inversión relativa en los distintos elementos del subfactor. Pero el subfactor es funcional y está definido (Observatorio de la Ciberseguridad , 2016).

Estratégico

Estratégico no significa importante; más bien, se trata de una selección. Al nivel nacional se han elegido las partes del subfactor que son clave, así como aquellas que son menos importantes para la organización/país en particular. Estas elecciones toman en consideración un resultado esperado, una vez implementado, que contiene circunstancias particulares y otros objetivos nacionales existentes (Observatorio de la Ciberseguridad , 2016).

Dinámico

Es el nivel donde se quiere llegar en este proyecto de investigación en todos los componentes de seguridad cibernética a nivel dinámico, existen mecanismos claros para alterar la estrategia en función de las circunstancias imperantes. Por ejemplo, la tecnología del entorno de amenazas, conflicto global, un cambio significativo en un área de interés (por ejemplo, la delincuencia cibernética o privacidad). Organizaciones dinámicas han desarrollado métodos para cambiar las estrategias, de acuerdo con una manera de "sentir y responder". La toma de decisiones rápida, la reasignación de los recursos y la atención

constante a los cambios del entorno son las características de este nive (Observatorio de la Ciberseguridad , 2016).

1. Política y estrategia
2. Cultura y sociedad
3. Educación
4. Marcos legales
5. Tecnologías (Observatorio de la Ciberseguridad , 2016)

Análisis cuantitativo y cualitativo del perfil del sistema de seguridad cibernética en Colombia

Dado el carácter multidimensional de las conclusiones y tendencias producto de la problemática en seguridad cibernética en el país, es importante focalizar la continuidad de los procesos de obtención de los objetivos y estrategias, ya que esto permite delinear y parametrizar la creación de una unidad nacional de seguridad cibernética en Colombia, basándonos en un análisis producto de un diagnostico situacional, donde se retoman sintéticamente de las cinco dimensiones, Política y estrategia, Cultura y sociedad Educación, Marcos legales, Tecnologías (Observatorio de la Ciberseguridad , 2016)en función del grado de aprovechamiento de las oportunidades que brinda el entorno, así como la capacidad de minimizar las amenazas.

Como resultado del proceso se obtuvieron los siguientes elementos significativos para el sistema de seguridad y defensa cibernética de acuerdo al observatorio de ciberseguridad en América latina y el Caribe.

1. **Dimensión política y estrategia Sistema de defensa y seguridad cibernética en Colombia**

   Para consolidar una unidad dedicada a la defensa de la seguridad cibernética lo primordial es establecer el área política y estrategia que determinaran los objetivos y habilidades entorno a la seguridad nacional, involucrando directamente la cibernética oficial o documentada (Observatorio de la Ciberseguridad , 2016) mediante la cual se divide en tres aspectos importantes en el que son; desarrollo de la estrategia, organización

y contenido de la misma, todo esto con base en el estudio hecho por el observatorio de la ciberseguridad en América latina y el Caribe.

Es importante resaltar que para Colombia desde la posesión de Juan Manuel santos calderón como presidente de la república en el año 2010, se plantea una política integral de seguridad y defensa para la prosperidad (Ministerio de Defensa Nacional , 2011) donde como estrategia propuso realizar un programa de ciberseguridad y ciberdefensa con el fin de desplegar habilidades y capacidades para contrarrestar todo tipo de retos a la seguridad derivados del espacio virtual. El diseño de una estrategia y una política contra el crimen y el terrorismo cibernético, así como la puesta en marcha del centro de respuestas a emergencias cibernéticas, son compromisos significativos. (Ministerio de Defensa Nacional , 2011)

1.1 Estrategia nacional de seguridad cibernética oficial o documentada.

Desarrollo de la estrategia	*nivel de madurez*	*establecido*
Organización	*nivel de madurez*	*formativo*
Contenido	*nivel de madurez*	*establecido*

1.2 Defensa cibernética

Estrategia	***nivel de madurez***	***formativo***
Organización	***nivel de madurez***	***establecido***
Coordinación	***nivel de madurez***	***formativo***

2. Dimensión de Cultura y sociedad Sistema de defensa y seguridad cibernética en Colombia

La mentalidad de seguridad cibernética en el país es escasa debido a que no se establecen programas de formación, acerca de la gestión de este riesgo, la mayoría de empresas colombianas las cuales manejan amplias bases de datos, como bancos, y universidades entre

otros, no saben proteger su información, por lo que es importante que se ejerza un control interno en las organizaciones con el fin de crear protocolos de seguridad que se encuentren plenamente establecidos, así mismo dentro de las empresas e instituciones públicas del Estado, para lo cual se deben establecer políticas de formación y capacitación entorno a generar mentalidad de seguridad cibernética, con el propósito de estar en situación a las nuevas amenazas de una comunidad global.

2.1 Mentalidad de seguridad cibernética

En el gobierno	*nivel de madurez*	*formativo*
En el sector privado	*nivel de madurez*	*formativo*
En la sociedad	*nivel de madurez*	*establecido*

2.2 Conciencia de seguridad cibernética (Observatorio de la Ciberseguridad , 2016)

Sensibilización	*nivel de madurez*	*establecido*

2.3 Confianza en el uso del internet (Observatorio de la Ciberseguridad , 2016)

En los servicios en línea	*nivel de madurez*	*establecido*
En el gobierno electrónico	*nivel de madurez*	*establecido*
En el comercio electrónico	*nivel de madurez*	*formativo*

2.4 Privacidad en línea (Observatorio de la Ciberseguridad , 2016)

Normas de privacidad	*nivel de madurez*	*establecido*
Privacidad del empleado	*nivel de madurez*	*establecido*

3. Dimensión de Educación en Sistema de defensa y seguridad cibernética en Colombia

Las capacitaciones o los procesos de formación en la educación en el área de ciberseguridad y ciberdefensa tanto en el área pública y privada no deben estar condicionados a factores externos, es por esto que en la actualidad existen algunas universidades que ofrecen especializaciones en seguridad informática y derecho informático, pero se ha identificado que la aceptación a este tipo de programas académicos en calidad de posgrado es prácticamente nula.

El resultado de esto, es que los interesados en estudiar especializaciones en ciberseguridad por lo general lo hacen en programas ofrecidos por centros de educación superior del exterior, es por esto que se deben fortalecer este tipo de proyecto curriculares a fin de que el desarrollo de educación de seguridad cibernética nacional experimente un interés e incremente el número de colombiano que deseen capacitarse en el tema dentro del país, así mismo ampliar la oferta mediante foros público-privados y centros de excelencia financiados por el gobierno, a fin de que se despierte interés acerca del tema.

Numerosas universidades, organismos policiales y de defensa y las empresas privadas ofrecen cursos y capacitaciones, incluyendo maestrías y programas de acreditación (Observatorio de la Ciberseguridad , 2016) El entrenamiento y formación de los funcionarios públicos y privados porque la escuela de administración publica la cual es la encargada de desarrollar programas de capacitación para funcionarios públicos para reaccionar ante un delito informático es deficiente.

3.1 Disponibilidad nacional de la educación y formación cibernética (Observatorio de la Ciberseguridad , 2016)

Educación	nivel de madurez	establecido
Formación	nivel de madurez	formativo
Desarrollo nacional de La educación de la seguridad Cibernética	nivel de madurez	formativo

3.2 Formación e iniciativas educativas Públicas y privadas (Observatorio de la Ciberseguridad , 2016)

Capacitación de los empleados

En seguridad cibernética nivel de madurez establecido

3.3 Gobernanza corporativa conocimiento y normas (Observatorio de la Ciberseguridad , 2016)

Comprensión de la seguridad cibernética

Por parte de las empresas privadas y estatales nivel de madurez formativo

4. Dimensión del Marco legal Sistema de defensa y seguridad cibernética en Colombia

Hay mecanismos de protección establecidos en un marco legal de seguridad de la información, sin embargo continúan falencias que tropiezan los procedimientos para responder oportunamente a incidentes y delitos cibernéticos.

El Congreso de la República aprobó la Ley de Inteligencia y contrainteligencia, estableciendo mecanismos de vigilancia y control para estas actividades. Así las cosas es un marco normativo que requiere ser más concreto para el ejercicio de la ciberseguridad y la ciberdefensa en Colombia.

4.1Marco jurídico de seguridad cibernética (Observatorio de la Ciberseguridad , 2016)

Debe haber un marco legal robusto donde se especifique uno a uno las falencias, dejando claro lo que sebe hacer para crear un marco legal y dinámico en materia de seguridad y confidencialidad donde converjan todas las instituciones públicas del estado en un enfoque de sinergia las sanciones deberían ser impuestas a las organizaciones que le den otro tipo de uso a las informaciones de su base de datos, en lo que concierne a la nómina, estructuras organizativas entre otros.

Para la seguridad de las TIC *nivel de madurez* *formativo*

Privacidad protección de datos *nivel de madurez* *establecido*

Y otros derechos humanos

Derecho sustantivo de Delincuencia cibernética	*nivel de madurez*	*establecido*
Derecho procesal de delincuencia Cibernética	*nivel de madurez*	*establecido*

5. Dimensión de tecnologías Sistema de defensa y seguridad cibernética en Colombia

5.1 Adhesión a las normas

Aplicación de las normas y Practicas mínimas aceptables	*nivel de madurez*	*formativo*
Adquisiciones	*nivel de madurez*	*formativo*
Desarrollo de software	*nivel de madurez*	*formativo*

5.2 organizaciones de coordinación de seguridad cibernética (Observatorio de la Ciberseguridad , 2016)

Centro de mando y control	*nivel de madurez*	*establecido*
Capacidad de respuesta a incidentes	*nivel de madurez*	*formativo*

5.3 respuesta a incidentes (Observatorio de la Ciberseguridad , 2016)

Identificación y designación	*nivel de madurez*	*formativo*
Organización	*nivel de madurez*	*formativo*
Coordinación	*nivel de madurez*	*formativo*

5.4 Resilencia de la infraestructura nacional (Observatorio de la Ciberseguridad , 2016)

Infraestructura tecnológica	*nivel de madurez*	*establecido*
Re- silencia nacional	*nivel de madurez*	*formativo*

5.5 protección de la infraestructura critica nacional (Observatorio de la Ciberseguridad , 2016)

Identificación	*nivel de madurez*	*formativo*
Organización	*nivel de madurez*	*formativo*
Planeación de respuesta	*nivel de madurez*	*inicial*
Coordinación	*nivel de madurez*	*formativo*
Gestión de riesgos	*nivel de madurez*	*formativo*

5.6 gestión de crisis (Observatorio de la Ciberseguridad , 2016)

Planeación	*nivel de madurez*	*formativo*
Evaluación	*nivel de madurez*	*formativo*

5.7 Redundancia digital (Observatorio de la Ciberseguridad , 2016)

Planeación	*nivel de madurez*	*formativo*
Organización	*nivel de madurez*	*formativo*

5.8 Mercado de la ciberseguridad (Observatorio de la Ciberseguridad , 2016)

Tecnologías de seguridad cibernética	*nivel de madurez*	*formativo*
Seguros de delincuencia cibernética	*nivel de madurez*	*formativo*

Conclusiones del nivel de madurez de la seguridad cibernética en Colombia

El nivel de madurez de la seguridad cibernética en Colombia se ubica en una etapa formativa y demarcada dentro de las cinco dimensiones planteadas por el observatorio cibernético para América latina y el Caribe, en la etapa formativa es fundamental estar dentro de la caracterización de un factor especifico de dichas dimensiones, permitiendo esto, que se de apertura a una nueva etapa en esta materia, en este nivel aún se presentan deficiencias en el tema tales como que aún se visualizan desorganizados, mal definidas o simplemente "nuevas" (Observatorio de la Ciberseguridad , 2016), dado que apenas se están moldeados los eventuales problemas que se potencializaran en un futuro no muy lejano, para lo cual ya existe una política nacional de seguridad cibernética CONPES 3701, pero esta no han sido tenida en cuenta en la mayoría de las dinámicas organizacionales, y para optimizar este proceso hay mucho trabajo por hacer ya que la madurez formativa solo es un planteamiento nuevo.

Otras dimensiones tienen su factores en etapa establecida como los son los elementos del subfactor que están delimitados y estableciendo aun. Sin embargo, no se ha considerado bien la asignación relativa de recursos (Observatorio de la Ciberseguridad , 2016). Esto quiere decir que ya hay una estructura organizativa en esos subtemas pero no hay recursos o inversión del gobierno la cual ayude a mejorar estas falencias, lo que deja vislumbrar un problema de toma de decisiones del actual gobierno colombiano.

Planteamientos que permitirían optimizar la seguridad cibernética en Colombia

Para poder establecer estrategias concretar que permitan consolidar una unidad de seguridad cibernética hay que tener en cuentas diversos aspectos que resultan fundamentales en la conclusión de los objetivos.

1. **Cuál es la fuente más probable de un ataque informático a la infraestructura del gobierno colombiano?**

De las potenciales respuestas que se generen a este tipo de pregunta, se pueden determinar planteamientos acerca de la vulnerabilidad de la infraestructura informática asi como determinar las debilidades que podrían convertir a Colombia en un blanco fácil ante

eventuales atacantes externos, en este contexto se pueden resaltar que los partidos políticos de oposición, organizaciones criminales que se familiarizan con grupos alzados en armas y asociaciones gremiales del país como los camioneros, productores de leche, entre otras sociedades sindicales estarían encabezando la lista de posibles víctimas así como de posibles victimarios.

Aunque una de las fuentes de un ataque informático sería dentro del mismo gobierno por un hacker infiltrado desde las mismas instituciones públicas del estado mediante riesgos informáticos como falta de protección de datos en el sentido que pueden entrar a un acceso no autorizado, el uso indebido de las redes sociales, y no a un especifico control de la seguridad de la información.

2. **Colombia posee una seguridad cibernética integrada mediante un proceso dinámico?**

El concepto integral tienen gran envergadura dado a todo lo que este término encierra, y para poder tener claridad en el caso de la cibernética integral, es importante detectar si la seguridad cibernética en Colombia tiene un plan de respuesta ante diferentes incidentes ya que esto comprometería cibernética integral, y de estar preparada para disminuir cualquier amenaza que se presente o mitigar el impacto ante cualquier ataque, para esto debe existir una coordinación entre todas agencias que tengan compromiso con la ciberseguridad, y de esta manera coordinar un plan de respuesta optimo con el objetivo de proteger la información del estado y ese equipo debe obedecer a una dirección idónea en el manejo de las TIC para contrarrestar este tipo de amenazas.

3. **Existe un análisis de riesgo de seguridad informática integral?**

Los riesgos en materia de cibernética son casi imperceptibles, lo que complica la tarea de realizar un análisis que permita establecer de manera concreta las potenciales debilidades del estado colombiano en el tema, para esto se hace una determinación del impacto, determinación del riesgo, valoración de las amenazas y tipos de amenazas a determinar.

Las amenazas mutan, así las cosas es fundamental que la seguridad de información que aplique el estado, se ajuste para mantener el ritmo y responder al dinamismo y necesidades cambiantes, de lo contrario, serán cada vez menos seguras y funcionales.

Del mismo modo, las agencias de seguridad informática deben trabajar con el propósito de mantener la seguridad cibernética actualizada a los nuevos requerimientos y exigencias del entorno global.

4. Existe un sistema de gestión de amenazas cibernéticas optimo?

Aunque está estipulado en el **CONPES 37014** LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA mediante el cual se establece el fomento de un sistema de gestión de conocimiento relativo a la ciberseguridad y ciberdefensa, orientado a la mejora de los servicios prestados por el colCERT no son dinámicos y por ende apenas está en una etapa de pro actividad por eso se hace perentorio crear las estrategias adecuadas para optimizar el sistema de gestión de amenazas cibernéticas.

5. Se puede hacer un plan de inteligencia de ataques cibernéticos?

La ausencia de un plan de inteligencia en seguridad informática conlleva a cometer errores para obtener la información solicitada, ya que no está unificada dentro de las mismas agencias de seguridad es por eso que acarrea las eventualidades que vamos a mencionar.

- No tomar un verdadero proceso de búsqueda para la información de amenazas cibernéticas lleva a realizar una y otra vez la misma tarea.
- Utilizar a varias personas en una búsqueda de información para la que no están debidamente capacitadas.

En estos procesos se pierde tiempo y dinero, por ende se gastan cantidad de recursos en planes perfectos, de seguridad cibernética como el plan estratégico, la planificación, la organización de las funciones entre otros pero luego es difícil conformar un plan que sistematice la obtención de información de la unidad nacional de seguridad cibernética lo cual ayudaría a facilitar todo tipo de riesgos.

6. **Como se pueden fijar las necesidades del programa de inteligencia de seguridad cibernética?**

A fin de poder plantear las necesidades fundamentales del programa de inteligencia y seguridad cibernética; debe apoyarse el programa en analistas especializados en el tema y dedicados a la inteligencia y asesores de índole externo quienes sean los que evalúan la información con el objetivo de dar credibilidad, a la seria exposición contra los ataques cibernéticos.

7. **Que es economía cibernética?**

Aunque la expresión economía cibernética pareciera estar contextualizada por la concreta definición de los dos términos, para efecto de la presente investigación hace referencia a los activos más importantes en la seguridad cibernética y su valor para los hackers, con esta información se podrá efectuar un plan para diseñar la seguridad cibernética en el país. Con el fin de que el valor de la información no corra ningún tipo de riesgo y se aproveche de manera asertiva.

8. **Como se pueden identificar los elementos claves para crear la unidad nacional de seguridad cibernética?**

Aunque la cibernética resulta ser muy compleja en el tema de seguridad, por la capacidad de las personas para alterar y modificar sistemas operativos en el caso de consolidar una unidad nacional de ciberseguridad, se puede establecer una política gubernamental que contribuya con los objetivos de unidad nacional para seguridad cibernética en Colombia, dichas políticas debe establecer derecho y deberes para los ciudadanos, y debe estar dirigida por el gobierno nacional para que interactúen los elementos claves para el desarrollo de la misma, y así pueda instituirse todo tipo de elementos donde el ataque cibernético no pueda prevalecer y pueda ser extinguido ya que este órgano gubernamental tomaría la iniciativa en esta materia.

9. Como llevar a cabo diferentes cursos de acción para optimizar la seguridad cibernética?

Pese a que la seguridad cibernética en Colombia no ofrece las garantías necesarias para catalogarse como un país pionero en el tema, si está en una constante búsqueda para conseguirlo.

Ante las acciones tomadas para la optimización de la ciberdefensa en Colombia, es plantear potenciales escenarios donde se puedan calcular el daño del ataque y se potencializa a que este será mucho mayor de lo esperado, de esta manera e pude prever, los mecanismo que permitan dar un manejo a los incidentes que se puedan presentar, que sea dinámico conlleve a visualizar las posibles soluciones, este orden de ideas se puede mencionar que a unidad nacional para la ciberdefensa podrá poner en acción los mecanismos adecuados.

Los stakeholders, deben ser identificados consisten en compradores, empleados, reguladores todos estos actores tienen un rol al establecer como es el estado de madurez de la seguridad cibernética y como maneja.

10. Como establecer un equipo de liderazgo para este tipo de proyectos?

Instaurar mecanismos de participación para involucrar e incluir las opiniones, quejas y preocupaciones de las agencias de seguridad cibernética del país, en sus planes de trabajo, de tal manera que se sientan parte de la visión y objetivos a emprender, y tomen una actitud no sólo cordial, sino que aporte con la prevención de todo tipo de amenaza que pongan en riesgo la información del país, igualmente esto converge para que todo el personal sin importar su clasificación, puedan sentirse parte de este proyecto significativo para el progreso del país.

El tema de la gestión del riesgo informático y que hacen parte de la compañía, deben emplear argumentos alternos para explicar a los grupos de interés que no ven sus requerimientos del todo solucionados" (Antonio, 2011, pág. 15), esto cómo otro tipo de recursos que pueden manifestar de que sí accedió a brindar solución a sus solicitudes quejosas a partir de los requerimientos efectuados por sus funcionarios. Hay que analizar la capacidad de respuesta ante ataques a la seguridad informática y el debido funcionamiento

del equipo de trabajo para responder oportuna y eficazmente a las inquietudes y requerimientos importantes, lo cual no significa necesariamente acceder a todo lo que ellos necesitan, sino atender de manera apropiada, expedita e inteligente a las demandas de los analistas de la seguridad informática.

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

La metodología de Análisis y Gestión de Riesgos de los Sistemas de Información debe soportarse en un marco de legalidad para lo cual es prudente consolidar un Consejo Superior de Administración Electrónica que permita minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones Públicas.

Una vez se establezca el Consejo Superior de Administración Electrónica se elabora un estrategia que promueva la utilización de estas tecnologías, como respuesta a la percepción de que la administración depende de forma creciente de las tecnologías de la información para el cumplimiento de su misión (Torres, 2010).

La razón de ser del mencionado consejo está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

Esto pude ser utilizado como metodología, y ser adaptada a las necesidades de trabajo para realizar un análisis de riesgos que sirva como diagnostico fiel a la empresa en estudio, para determinar su situación actual con respectó a la seguridad informática.

Capítulo Tres; Estructura del sistema nacional de seguridad cibernética

La ciberseguridad es un desafío para la sociedad como un todo y necesita una respuesta que surja de la cooperación entre los diversos actores, Colombia orientó este tema hacia un marco normativo, el cual se soporta en el Código Penal en 2009 mediante la Ley 1273 y el Código de Procedimiento Penal en 2011 mediante la Ley 1453. Ley 527 de 1999 "Comercio Electrónico'. Por lo anterior la ley sustantiva parece estar en amplia armonía con los estándares

internacionales, es decir, con el Convenio de Budapest. Disposiciones de derecho procesal más específicas pueden ser necesarias, incluyendo las enfocadas a la rápida conservación de datos. (Secretaría de Relaciones Exteriores, 2014) Se requiere que este marco normativo sea más dinámico para que todas las instituciones públicas del estado puedan diseñar un plan de acción acorde a las necesidades de la unidad nacional de seguridad cibernética, con el fin de crear una sinergia acorde a los más altos estándares de sistemas de seguridad cibernética en el mundo, la gestión de este organismo será defender la esfera civil de amenazas cibernéticas, así mismo cimentar y preservar la fortaleza de la infraestructura nacional de Colombia en aras de llegar a ser líder mundial en esta materia con el fin de proteger de distintos ataques tanto a ciudadanos como instituciones públicas del estado.

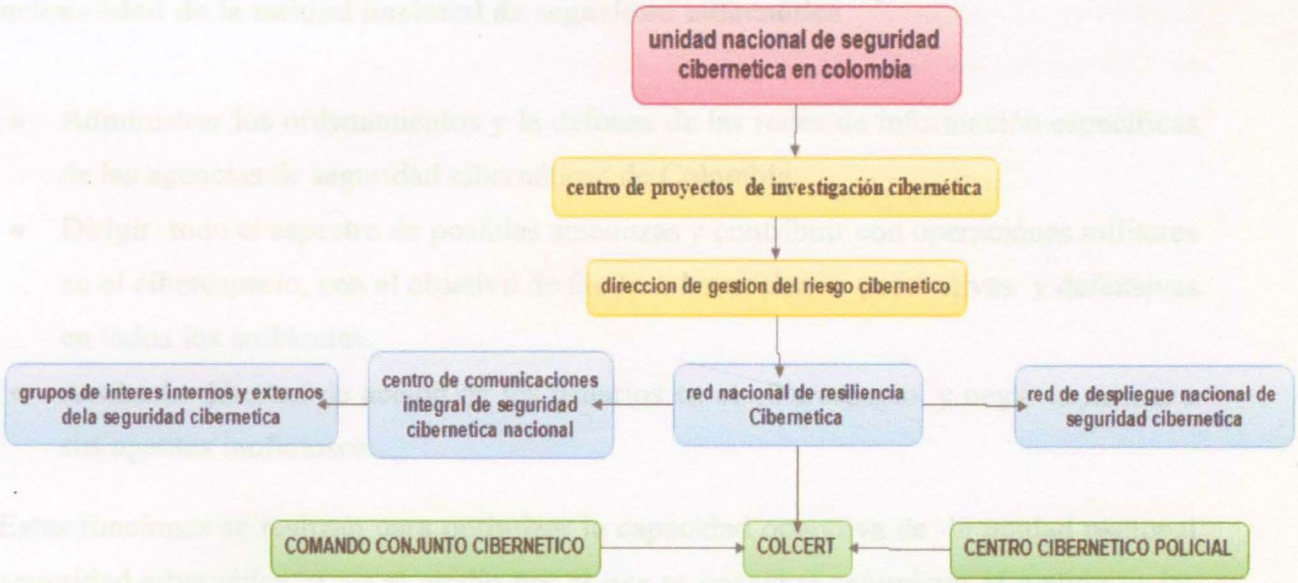


Imagen 6; Organigrama uno de la unidad nacional de seguridad cibernética en Colombia fuente edición propia

En el organigrama de la imagen 6, se establece la estructura jerarquita de una unidad nacional de seguridad cibernética, planteando un centro de proyectos de investigación cibernética este organismo adscrito a la unidad nacional tendrá como función realizar todo tipo de tendencias en seguridad cibernética, para retroalimentar a las demás agencias de seguridad cibernética , la dirección de gestión del riesgo cibernético, elaborara anualmente los planes de acción y contingencia así como la matriz de riesgos de tal manera que proyecte

su funcionalidad desde la capacitación a los funcionarios públicos y ofrecer formación en seguridad cibernética.

Misión de la unidad nacional de seguridad cibernética colombiana

Ejecutar labores de protección, prevención, promoción concerniente a la ciberdefensa militar en las redes y sistemas de la información y telecomunicaciones de las Fuerzas Armadas y otros organismos del estado así como contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la defensa y seguridad Nacional.

Funcionalidad de la unidad nacional de seguridad cibernética

- Administrar los ordenamientos y la defensa de las redes de información específicas de las agencias de seguridad cibernéticas de Colombia.
- Dirigir todo el espectro de posibles amenazas y contribuir con operaciones militares en el ciberespacio, con el objetivo de facilitar las acciones preventivas y defensivas en todos los ambientes.
- Avalar la libertad de acción de los usuarios en el ciberespacio, y negar la misma a sus agentes inoficiosos.

Estas funciones se realizan para optimizar la capacidad operativa de la unidad nacional de seguridad cibernética, y es el medio por el que se consigue centralizar el mando de las operaciones en el ciberespacio, fortaleciendo e integrando las capacidades del Ministerio de Defensa Nacional en el ciberespacio, ya que reúne todas las cibercapacidades existentes, creando una sinergia que no existía hasta ese momento.

Un sistema informático de coordinación entre Agencias de Seguridad es precisamente lo que se pretende desarrollar en este proyecto de investigación realizar un compendio, de modo efectivo y ágil con el propósito de que toda la información la cual sustraigan todas las Agencias sobre un caso concreto ayuden a tomar decisiones y medidas de respuesta con el objetivo de poder ofrecer una línea de defensa contundente.

Plan de acción para optimizar la unidad nacional de seguridad cibernética

Este plan de acción lo que pretende es estar dentro de un ámbito de mejora continua con el fin de que la seguridad cibernética en Colombia cobre mayor importancia para esto se debe desarrollar el uso oficial de las TIC como parte de la política de Colombia se incrementa la competitividad en las compañías de prestación de servicios del mismo modo se debe auxiliar a las empresas locales de tecnologías de la información, con el fin de fomentar una cultura sobre estructura y desarrollo organizacional, así mismo apoyo político por parte del gobierno nacional invirtiendo en personal experto en la materia bien informado, los cuales sean influyentes e importantes en comunidades internacionales, un musculo financiero por parte del estado colombiano sólido, mejorar la eficiencia de la red, soluciones a los problemas de infraestructura digital, Para tener éxito en materia de seguridad cibernética es indispensable capacitar a los usuarios de plataformas hogareñas con el fin de establecer higiene cibernético.

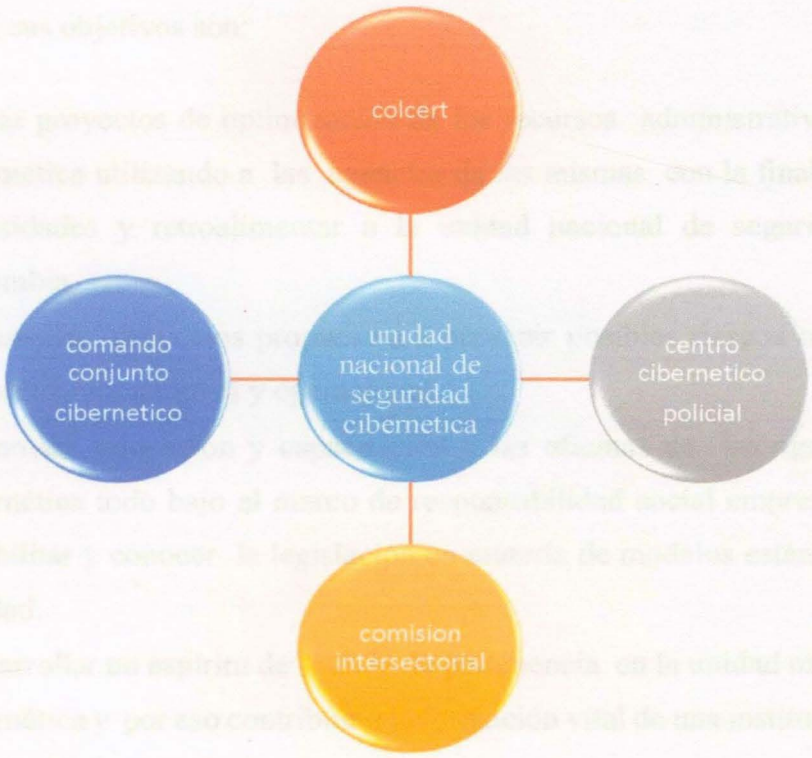


Imagen 7; Sinergia de la unidad nacional de seguridad cibernética colombiana fuente edición propia

La imagen siete se muestra la sinergia de la unidad nacional de seguridad cibernética en Colombia mediante la cual se aplicara una estrategia siguiendo con los principios y directrices de la política integral CONPES 3701 está política, ejercida por el gobierno nacional no se deben limitar al ámbito informático, sino que necesitan extenderse a las redes comerciales, controladas por la unidad nacional de seguridad cibernética. Para ello es fundamental establecer una hoja de ruta con el propósito de Evaluar el nivel de la seguridad frente a los riegos y vulnerabilidades cibernéticos en Colombia.

Administración de la seguridad cibernética

A fin de tener una administración optima de la seguridad cibernética se debe establecer una fuerza de trabajo capacitada y disciplinada direccionada al tema administrativo y organizacional, en el marco de modernización y desarrollo de la fuerza pública crear todo tipo de mecanismo que contribuyan a instaurar una estructura de organización sólida en materia de seguridad cibernética no solo en el campo administrativo sino también en lo operacional, sus objetivos son:

- Iniciar proyectos de optimización de los recursos administrativos de la seguridad cibernética utilizando a las agencias de las mismas con la finalidad de conocer las necesidades y retroalimentar a la unidad nacional de seguridad cibernética en Colombia.
- Desarrollar proyectos propuestos a prevenir posibles riesgos organizacionales en materia administrativa y operacional.
- Promover educación y capacitación a las oficinas de las agencias de seguridad cibernética todo bajo el marco de responsabilidad social empresarial con el fin de posibilitar y conocer la legislación en materia de modelos estándares de control de calidad.
- Desarrollar un espíritu de sentido de pertenencia en la unidad nacional de seguridad cibernética y por eso contribuir a la formación vital de una institución que esté acorde a todos los marcos de trasparencia.

La administración de la seguridad cibernética juega un rol muy importante, su eficiencia y validez, es producto de la dirección, habilidades y estrategias que se utilicen todo esto dependerá del trabajo final, y permitirá medir los resultados obtenidos.

Así mismo la delimitación administrativa de la unidad nacional de ciberseguridad, delimitara cada proceso de una forma sistemática como toda ciencia, inicia paso a paso, para que el producto y el proyecto converjan en uno mismo, con el fin de estar conexo de manera adecuada con los demás procesos, que suministra la coordinación deseada.

En la estructuración de la parte administrativa es importante apoyarse en la Guía del PMBOK del Project Management Institute donde se describe el entorno integrador de la dirección de proyectos, que requiere que el Grupo de Procesos de supervisión, Monitoreo y Control y el resto de Grupos de Procesos desplieguen todo tipo de actividades uno sobre los otros de manera retributiva o mutua (Mendoza, 2014).

La combinación de la administración de la seguridad cibernética obedece a especialidades muy particulares que ayudan a determinar una representación holística porque determina características de unificación, consolidación, comunicación y actividades decisivas para que el proyecto se lleve a cabo de manera controlada, de modo que se cumpla con los requisitos o parámetros exigidos, y se pueda establecer un departamento administrado de la unidad de seguridad cibernética.

Este departamento administrativo se requiere no solo trabajar en una especialidad si no apoyarse mutuamente con los procesos de las otras áreas de conocimiento, de modo que el trabajo resulte en la entrega del alcance del producto exigido por la unidad nacional de seguridad cibernética en Colombia Los esfuerzos de cada miembro de la dirección deben llegar a tener un grupo de alto desempeño y liderazgo organizacional de tal manera que se convierta en un soporte fundamental de la Unidad de Seguridad Cibernética de Colombia.

Tomar decisiones a lo largo de cada proyecto es totalmente importante, pero para tomar ese tipo de acciones se debe estar asesorado, suponiendo que para esto hay que tener la disposición con el fin de aceptar todo tipo de recomendaciones asertivas.

Por otro lado un departamento administrativo toma relevancia si se proyecta a desarrollar un ambiente de mejoramiento continuo en la optimización de servicios y procesos, los cuales deben estar plantados desde el análisis de las diferentes perspectivas que se puedan presentar y direccionado a la sugerencia de potenciales soluciones de los problemas por la dirección de administración del riesgo del Ejército Nacional, la cual es vital en un mundo altamente competitivo ya que se debe actuar bajo estándares internacionales.

Es fundamentar tener en cuenta que un gerente de proyectos es la pieza fundamental en el engranaje empresarial porque pone en funcionamiento toda la estructura organizacional de la compañía debido a sus conocimientos y su formación personal, para así mismo poder incorporar clientes potenciales todo esto bajo una visión integradora, hace que su equipo de proyecto sea el más organizado porque evalúan contingencias, analizan riesgos, elaboran procesos todo esto bajo la supervisión, monitoria y control.

Para planificar un proyecto debe establecerse una reunión con el objetivo de unificar un argumento o criterio organizacional de tal manera que se puedan instituir grupos de trabajo con la condición de designarlos en el área de conocimiento específica, así mismo ir en una sola línea de trabajo, tener la habilidad para enfrentar cualquier cambio o reto con su equipo de proyecto.

La unidad nacional de seguridad cibernética debe Inspeccionar y actualizar las políticas, y estándares de seguridad, todo esto para Implementar un sistema de gestión de la seguridad de información (SGSI). La importancia de este organismo gubernamental es ejercer un control eficiente de los casos conocidos a nivel global e interno y los procedimientos de respuesta a incidentes que han tenido aquellas agencias de seguridad extranjeras para un óptimo desempeño. Así mismo es importante también implementar controles de seguridad cibernética, analizar la prevención de pérdida de datos y programa de gestión de identidades y de accesos. Instaurar los procedimientos de respuesta de incidentes, con el ánimo de originar pruebas de penetración de la red.

Delimitación legal de la Unidad de Seguridad Cibernética.

Aunque la consolidación de esta una unidad encargada de la seguridad cibernética sería una entidad gubernamental, estaría subordinada al comando general de las FFMM, para lo cual necesita enmarcarse en lo parámetro de cada fuerza, para el caso del Ejercito Nacional de Colombia, debe incluirse en La Guía de Planeamiento Estratégico (GPE), que es uno de los documentos rectores para la definición y orientación del planeamiento estratégico de la Fuerza al 2030 (Ejercito Nacional de Colombia , 2015). De tal manera que permita la articulación de las políticas propuestas por el actual gobierno, que se ajuste a los parámetros proyectado por la institución como los son el Plan de transformación del Ejercito Nacional al 2030, el plan estratégico de las FFMM, Guía de aplicación del Plan Estratégico – GAPE 2015 – 2018 y Plan de Guerra "Espada de Honor", todo esto se encuentra soportado por la constitución política de Colombia en el artículo 217, y regidas por las Política de Defensa y Seguridad para la Nueva Colombia.

Capítulo Cuatro; Preparación y capacitación del sistema nacional de seguridad cibernética

Con el fin de dar una solución eficaz, que ayude a mejorar la planeación estratégica que implica el riesgo global en el tema de ciberdefensa, se pueden establecer lineamientos sólidos que ayuden a fortalecer a Colombia en materia de seguridad cibernética, como una estrategia eficaz, y probable solución ante este flagelo, utilizando herramientas tecnológicas que permitan que las fuerzas militares establezcan la creación de un centro de proyectos de investigación cibernética que soporte la unidad nacional de ciberseguridad, direccionada hacia la implementación de todo tipo de proyectos en pro de la defensa ciberespacial, uno de los miles ejemplos que se pueden hacer en el centro de investigación cibernética es, un radio el cual posea un software que le permita suministrar información 100% segura, se puedan enviar fotos y documentos reservados dentro de este radio, ya que actualmente los radios de comunicación militar utilizan frecuencias compartidas por radioaficionados civiles que pueden ser interceptadas fácilmente por hackers o por personal que manejen los radio scanner.

Con base en lo anterior resalta la importancia de generar todo tipo de hábitos que ayuden a resolver la diversidad de problemas que enfrentan la seguridad cibernética, y, la economía

digital para lo que es necesario un conjunto de respuestas innovadoras. El Informe Global de Tecnología de la Información pone de relieve varias políticas gubernamentales sencillas que pueden ayudar a los residentes a aumentar su acceso a Internet. (TIC, 2012). Impartir programas de educación cibernética por parte de la escuela de administración pública con el objetivo de que los funcionarios públicos estén capacitados y mejores sus hábitos de utilizar la red y el ciberespacio.

La ciberdefensa es un tema relativamente nuevo e inexplorado a nivel mundial, puesto que aunque el episodio entre Rusia y Estonia, prendió las alarmas aún no se han presentado guerras en el área que permitan evaluar los alcances de en el área, pero actualmente hay varios países que adelantan investigaciones que permitan mitigar los impactos causados en el hipotético caso que se presenten

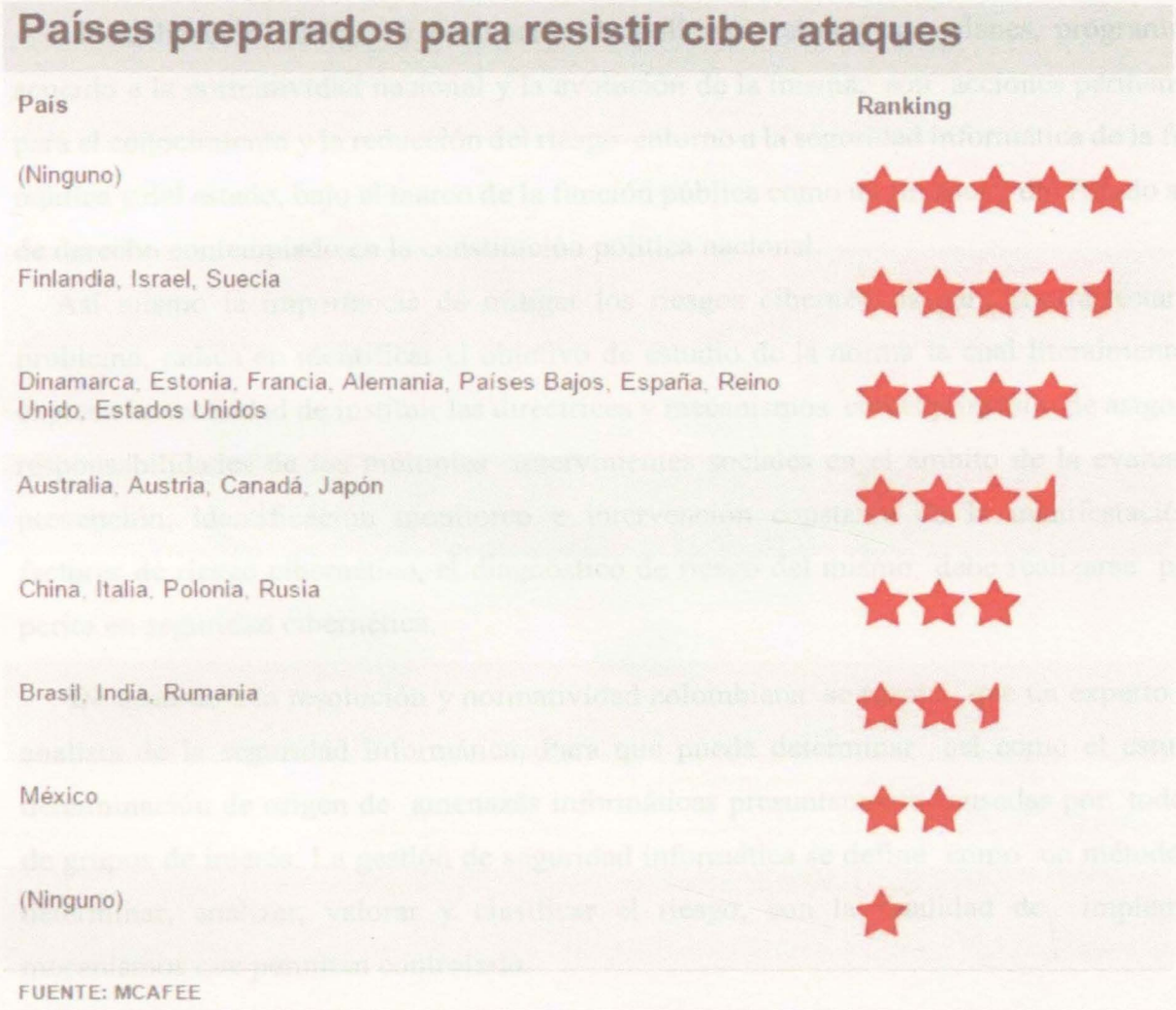


Imagen 8; Países preparados para resistir un ciberataque fuente tomada por: McAfee (cruz, 2012)

En esta imagen se puede observar que son muy pocos los países preparados para un ataque cibernético por ende la importancia de realizar todo tipo de buenas prácticas organizacionales y operacionales con el propósito de optimizar la seguridad cibernética en Colombia contribuiría a la eficiencia de la misma, la capacitación y preparación es el baluarte de apoyo de la unidad nacional de seguridad cibernética en Colombia. En el caso específico de Colombia aunque ha dado grandes avances en el tema aún falta concretar estrategia que eviten una crisis en caso de ser atacado desde el ciberespacio.

Gestión en seguridad informática

La realización, alcance y evaluación de políticas, estratégicas, planes, programas de acuerdo a la normatividad nacional y la evolución de la misma, son acciones permanentes para el conocimiento y la reducción del riesgo entorno a la seguridad informática de la fuerza pública y del estado, bajo el marco de la función pública como un fin social del Estado social de derecho contemplado en la constitución política nacional.

Así mismo la importancia de mitigar los riesgos cibernéticos para contrarrestar este problema, radica en identificar el objetivo de estudio de la norma la cual literalmente nos expresa la necesidad de instituir las directrices y mecanismos con el propósito de asignar las responsabilidades de los múltiples intervinientes sociales en el ámbito de la evaluación, prevención, identificación monitoreo e intervención constante de la manifestación en factores de riesgo cibernético, el diagnóstico de riesgo del mismo debe realizarse por un perito en seguridad cibernética.

De acuerdo a la resolución y normatividad colombiana se razona que un experto es un analista de la seguridad informática. Para que pueda determinar así como el estudio y determinación de origen de amenazas informáticas presuntamente causadas por todo tipo de grupos de interés. La gestión de seguridad informática se define como un método para determinar, analizar, valorar y clasificar el riesgo, con la finalidad de implementar mecanismos que permitan controlarlo.

Hablar de gestión del riesgo en materia e ciberdefensa implica ahondar en un tema poco explorado, pero que requiere una parametrización inmediata que no permita que los sistemas de seguridad del Estado sean vulnerados, responsabilidad que se le atribuye las FFMM, por su misión constitucional establecida en la constitución política de Colombia de 1991.

Esto lo incluye en el plan nacional de desarrollo PND, el cual se focaliza en tres pilares fundamentales, paz, equidad y educación, pero para poder cumplir con estos tres objetivos es necesario que se garantice la seguridad nacional, desde todo punto de vista.

Imagen 9; fases de la gestión del riesgo fuente edición: wordpress (Rojas, 2012)

En la imagen nueve la gestión del riesgo informático se sujeta a cuatro políticas para su debida aplicación:

- **Análisis de seguridad informática**: Establece los mecanismos de un sistema que requiere protección, sus vulnerabilidades y las amenazas, con el resultado de revelar su grado de riesgo y estado de madurez.
- **Clasificación del riesgo informático**: Estipula si los riesgos enfrentados y los demás riesgos son tolerables con base a esto se puede maximizar y enfrentar toda amenaza a la información.
- **Reducción**: Define e implementa las medidas de protección. Además sensibiliza y capacita los usuarios conforme a las medidas.
- **Control**: Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento.

Todo el proceso está basado en políticas de seguridad, normas y reglas institucionales, que forman el marco operativo del proceso, en seguridad informática con el propósito de definir buenas prácticas:

- Potenciar las capacidades institucionales, reduciendo la vulnerabilidad y limitando las amenazas con el resultado de reducir el riesgo.
- Orientar el funcionamiento organizativo y funcional.
- Garantizar comportamiento homogéneo.
- Garantizar corrección de conductas o prácticas que nos hacen vulnerables.
- Conducir a la coherencia entre lo que pensamos, decimos y hacemos

La fuerza pública debe instaurar los mecanismos para optimizar la unidad nacional de seguridad cibernética en Colombia el cual involucra a todas las unidades militares del país y a las instituciones públicas del estado a contribuir en la estructura organizacional en ámbitos administrativos y operacionales, del mismo modo sirve como un instrumento de participación, en el cual debe incluir las opiniones, quejas y preocupaciones de las demás agencias de seguridad cibernética a nivel nacional para plasmarlas en sus planes de trabajo, y planes de mejoramiento institucional, de tal manera que se sientan parte de la visión y objetivos, de la unidad nacional de seguridad cibernética y tomen una actitud no sólo cordial sino puedan aportar con el fin de prevenir todo tipo de riesgo administrativo y operacional al que se pueda afrontar la instituciones, igualmente esto converge para que todos los demás participes de estos procesos sin importar su grado, y de esta manera puedan sentirse parte de la unidad nacional, porque el seguimiento a los procesos de acción no solo seria de los altos mando militares, si no de cualquier miembro de la institución mediante un proceso de mejora continuo.

Cabe resaltar que aspectos importantes y casi fundamentales en todas las políticas de seguridad, se deben destacar tanto las capacidades del personal como la eficiencia de los recursos para generar confianza en la ciudadanía. Así mismo las relaciones con el público son trascendentales en este proceso, dado debe existir entre los miembros de la organización, y los grupos de interés internos y externos lineamientos de cooperación para que así se pueda alcanzar los mejores resultados es un proceso progresivo en aras de cumplir los objetivos propuestos en la unidad nacional de ciberdefensa, realizando una proyección que permita

crear futuros escenarios con el propósito de mejorar día a día, para que quede establecido como una cultura organizacional y hábito.

Imagen 10, ciclo de mejora continua del proceso fuente tomada por: calidad y gestión (learning, 2015)

La mejora continua va de la mano con el compromiso y el aprendizaje incesante, tonándose en características fundamentales para obtener un seguimiento de una filosofía de gestión, y así poder incluir la participación activa de la comunidad en general como pilar que sustente la consolidación de la unidad nacional de ciberdefensa.

En este contexto es importante identificar desde la administración del riesgo informático los ciclos del proceso de mejora continua, los cuales son fundamentales para el cumplimiento de los objetivos institucionales.

La mejora continua se logra con la asociación de ciertas reglas a los procesos institucionales de desarrollo que nos permitan **identificar** aquello que se hace mal para poder **corregirlo** y si es posible replantear el proceso para **prevenirlo** en el futuro. Normalmente

el proceso de mejora continua se aplica de manera cíclica, lo que permite aprender y/o mejorar algo nuevo en cada ciclo (Sevilla, 2011).

Estas buenas prácticas optimizan el desarrollo organizacional de la misma con la finalidad de contribuir a mejorar el rendimiento con la aplicación correcta de la administración de la seguridad cibernética.

Programa de inteligencia artificial una amenaza cibernética

Actualmente existe procesos de automatización donde unifica la información, pero dichos procesos son efectivos por la intervención humana, ósea que por avanzado que parezca el software debe estar controlado por un ser un humano, entonces la inteligencia artificial no posee la potestad de controlar maquinas por sí misma, para que el programa de inteligencia ante amenazas cibernéticas sea efectivo, deberá ser ejecutado rápidamente por analistas de seguridad cibernética. Existe una variedad de servicios de inteligencia ante amenazas cibernéticas disponibles y estos deben ser evaluados específicamente para los requerimientos, necesidades y madurez de la organización (Observatorio de la Ciberseguridad , 2016).

La potenciación del conocimiento es uno de los elementos clave de la sociedad y así mismo de la unidad nacional de seguridad cibernética que estaría al servicio del pueblo colombiano con el objetivo de lograr la ventaja competitiva en la seguridad de la información en un período o ámbito prospectivo que estén acordes con las exigencias en un mundo globalizado. La gestión de la información y del conocimiento, se han desarrollado para manejar organizaciones, que esencialmente optimizan los servicios.

El conocimiento, ha sido considerado auténticamente un bien privado, con el transcurrir del tiempo ha comenzado a convertirse en un bien público, ya que contribuye a socializar la cultura gracias al apoyo de las nuevas tecnologías de información y de comunicación en las concepciones sobre los recursos humanos y la potenciación de conocimiento, se deben promover el crecimiento institucional en todas las direcciones donde apunte la sociedad para contribuir a la seguridad y convivencia.

El programa de inteligencia ante amenazas cibernéticas también puede llegar a ser muy útil al momento de dar valor a la gestión de riesgo, y por su puesto al identificar las potenciales deficiencias de la red actual, lo cual debe dar lugar a cambios en el proceso que permitan la normal vinculación al programa propuesto. (Advisory Services, 2015).

La importancia de identificar los grupos de interés en la seguridad informática

La seguridad cibernética es un tema que aunque no está muy explorado si es requerido no solo por el sector defensa sino también por el sector empresarial entre otros, lo que permite que las políticas de seguridad en cibernética sean con proyección no solo a presentar un servicio al Estado si no también que permita proteger la comunidad en general y esto en disposición de investigar todos los delititos cometidos desde el ciberespacio, para esto se puede considerar como apoyo el equipo de gestión de stakeholders, como fundamento de las organizaciones que requieran proteger la cualquier tipo de información que consideren que pueden ponerlo en riego, teniendo en cuenta esto, es importante que el personal este calificado para que pueda identificar los eventuales riesgo de interés tanto del estado como de cada uno de los colombiano, de forma óptima, ya que el personal es el recurso humano fundamental de toda empresa.

Se dice que es el activo más valioso. La compañía puede tener un producto original o un servicio excelente, pero es la gente mediante sus virtudes profesionales y sus principios morales y éticos (Santiesteban, 2007), por lo que la capacitación del personal que integre la unidad nacional deben cumplir con unos estándares establecidos, y deben direccionarse a la consecución de la confianza del cliente en este caso de la población civil y del gobierno nacional y hacer que vuelva a requerir de sus servicios con satisfacción seguirían obteniendo credibilidad. Es importante que en el momento de determinar las funciones de los miembros de la unidad nacional de ciberdefensa se tenga claridad en las capacidades indíqueles de cada uno de los miembros para que se ubique como expertos en su campo de acción.

Esta aclaración se hace dado que en las entidades gubernamentales colombianas suele evidenciar en muchas ocasiones las deficiencias que presentan los equipos de trabajo, esta responsabilidad se le atribuya a que estos son conformados por personas que asumen roles diversos roles sin tener la preparación necesaria, o están preparados para otro tipo de

actividad sin tener el conocimiento que el área de trabajo que se requiere; es así como pueden verse equipos conformados por trabajadores sociales que terminan asumiendo el papel de asesores jurídicos, abogados asumiendo el rol que le compete a comunicadores y comunicadores asumiendo el papel que le compete a trabajadores sociales. Permitir situaciones como esa en la gestión y compromiso de stakeholders externos ha generado errores de planeación y ejecución, falta de entendimiento con los grupos de interés e incumplimiento de los objetivos planteados.

El objetivo primordial de la unidad nacional de seguridad cibernética que haría parte del ministerio de defensa seria el ente garante de la seguridad a la infraestructura de la información, con el fin de que los datos estén debidamente protegidos y se pueda confiabilidad de información, para que de esta manera se pueda invertir en las fallas como son; tecnología, y personal calificado, Teniendo en cuenta que ese es el ámbito de ejecución empresarial donde más aparecen las fallas, los directivos deben orientarse en dichos aspectos y de disponer de la mayor parte de su tiempo y recursos, a mencionadas áreas; sin embargo, como ya se puede concluir la gestión y compromiso de stakeholders externos demanda de tiempo, compromiso y recursos, componentes que no suelen ser tenidos en cuenta en los altos niveles directivos. Se hace importante que directivos con poder de decisión financiera se impliquen en el asunto de gestión social, estén al tanto del mismo y ayuden a asegurar la alineación y compromiso.

Conclusiones

El ciberespacio es la red interdependiente de los fundamentos tecnológicos mediante la cual se caracteriza la información, que involucra internet y otras redes de comunicación telegráfica, procedimientos computacionales, ordenadores totalizados y controladores de industrias críticas. Y es mediante la cibernética que se consiente que personas e instituciones intervengan e intercambien información. El "nuevo dominio de los computadores" ha facilitado y acelerado la velocidad de las comunicaciones alrededor del mundo, por lo cual se ha convertido en un factor esencial para el funcionamiento de la economía, la política y la cultura de todas las naciones del planeta

La creación de la Unidad Nacional de Seguridad Cibernética por parte del Ejercito Nacional de Colombia aportaría de manera directa en el cumplimiento del rol constitucional de las FFMM establecido en la constitución política de Colombia en el artículo 217, dado que los riesgos generados en el tema parecieran ser imperceptibles pero persistentes y podrían vulnerar la Seguridad y Soberanía nacional. Pero dicha unidad debe estar en marcada en el Plan estratégico institucional 2015 -2018.

Es importante tener en cuenta que el tema de seguridad cibernética, es contemporáneo y hasta ahora se inicia las fases exploratorias y aunque en el mundo se han evidenciados ciberataque, hasta la fecha no se experimentado las ciberguerras, para poder medir la magnitud de los impactos acusados, a la seguridad nacional de un país.

La Unidad Nacional de Seguridad Cibernética tendría como objetivo principal proteger y asegurar los datos del estado con el propósito de investigar delitos cibernéticos complejos, y sanear enfoques de detección y respuesta con mecanismos óptimos de protección, así mismo analizar el nivel de madurez de la seguridad cibernética en Colombia a fin de dar un enfoque dinámico a la misma.

Cabe resaltar que de darse la etapa posbélica, pueden llegar a presentarse una eventual ciberguerra, si se consideran que se entregan hay dejación de armas, la disidencia de los grupos armados pueden visualizar esto como un posible mecanismo para desestabilizar el Estado.

El principal obstáculo para la consolidación de la Unidad Nacional de Seguridad Cibernética, es la asignación presupuestal, ya que la inversión es considerablemente amplia puesto se requiere adquisición de equipos tecnológicos y capacitación de personal que integraría la unidad.

En el transcurso de las dos últimas décadas, se han evidenciado diversas amenazas en contra de la infraestructura interconectada. Esta es altamente vulnerable y si se atenta contra ella, puede llegar a paralizarse completamente un país. Las amenazas cibernéticas tienen una connotación sustancialmente diferente a la de otras amenazas a la seguridad nacional; dado que éstas pueden tener diferentes objetivos.

Recomendaciones

Colombia requiere responder a la necesidad de crear una alta comisión para estudiar la estrategia de seguridad cibernética del país, en conjunto los ministerios de Defensa Nacional, TIC y Justicia, y consultar con expertos nacionales para elaborar un diagnóstico de la actual situación del país en materia de Ciberseguridad y ciberdefensa, apoyados en los conocimientos pertinentes en la experiencia en Ciberseguridad que han desarrollado otros países del mundo que han sido pioneros en materia de Ciberseguridad, lo que sugiere el fortalecimiento y consolidación de vínculos tanto bilaterales como multilaterales.

Referencias

Advisory Services. (24 de agosto de 2015). *Perspectivas sobre Gobierno, Riesgo y Cumplimiento.* Obtenido de Adelántese a los delitos cibernéticos: http://www.ey.com/Publication/vwLUAssets/Encuesta_global_de_seguridad_de_informaci%C3%B3n_2014/$FILE/EY-encuesta-global-de-seguridad-de-informacion-2014.pdf

Antonio, V. (2011). *La responsabilidad social empresarial en america latina.* Washintong: Banco interamericano de desarrollo.

consultors, A. (2009). competitividad y desarrollo empresarial. *liderazgo y gestion empresarial*, 11.

cruz, j. g. (2012). la cibernetica en el estudio interdisciplinario. En j. g. cruz, *la cibernetica en el estudio interdisciplinario* (págs. 12-21). lima: publicaciones de seguridad de la informacion. Obtenido de la cibernetica en el estudio interdisciplinario.

diario, e. n. (13 de marzo de 2016). Solo 6 países en América Latina y el Caribe tienen estrategias contra ciberataques. *el nuevo diario*, pág. 1. Obtenido de http://www.elnuevodiario.com.ni/suplementos/tecnologia/387570-solo-6-paises-latina-caribe-tienen-estrategias-cib/

Ejercito Nacional de Colombia . (2015). *PLAN ESTRATÉGICO 2015 - 2018.* Bogota : Comando General de las Fuerzas Militares .

El Espectador . (13 de octubre de 2015). Presupuesto de la Nación para 2016 tendrá capítulo del posconflicto. *El Espectador*, págs. 02-03.

el pais . (12 de agosto de 2015). Qué papel van a desempeñar las Fuerzas Militares en el postconflicto? *Qué papel van a desempeñar las Fuerzas Militares en el postconflicto?*, pág. 1.

Espectador, E. (13 de enero de 2016). Credicorp Capital y Sura Asset Management crearon fondo privado para financiar vías 4G. *El Espectador* , pág. 01.

FFMM. (2012). *informe de gestion 2012.* Bogota: Fuerzas Militares de Colombia.

Heraldo, E. (15 de octubre de 2015). Gobierno destina $10 billones para posconflicto. *El Heraldo*, págs. 10-11.

Krick, T. (2006). El compromiso con los stakeholders. *MANUAL PARA LA PRÁCTICA DE LAS RELACIONES CON LOS GRUPOS DE INTERES*, 12.

learning, l. h. (2015). Mejora continua en desarrollo. *innovacion y emprendimiento*, 11. Obtenido de http://comunidad.iebschool.com/fafolkie/2014/05/21/mejora-continua-en-desarrollo-del-software-por-donde-empezar/

Madrid, J. E. (12 de abril de 1997). *Razon y palabra* . Obtenido de Razon y palabra : http://www.razonypalabra.org.mx/mcluhan/aldjav.htm

Mendoza, L. I. (12 de Junio de 2014). Liderazgo Gerencial Transformacional. Bogota, Colombia.

Ministerio de Defensa Nacional . (2011). *Política Integral de seguridad y defensa para la prosperidad.* bogota: gobierno nacional.

Observatorio de la Ciberseguridad . (10 de enero de 2016). *observatorio de ciberseguridad para america latina y el caribe.* organizacion de estados americanos: banco interamericano de desarrollo. Obtenido de observatorio de ciberseguridad .

portafolio. (2015). Con los proyectos 4G, Colombia será más competitiva. *portafolio*, 1. Obtenido de http://www.portafolio.co/economia/finanzas/proyectos-4g-colombia-sera-competitiva-34346

Rojas, S. C. (2012). *ciberdefensa y ciberseguridad una nueva prioridad para las naciones.* bogota: universidad militar nueva granda. Obtenido de http://repository.unimilitar.edu.co/bitstream/10654/12937/1/CIBERDEFENSA%20Y%20CIBERSGURIDAD.pdf

sandroni, A. (2010). prevencion de guerras ciberneticas. En A. sandroni, *prevencion de guerras ciberneticas* (págs. 12-19). caracas: Lic. en Derecho por la UMinho.

Santiesteban, A. y. (2007). *Valores y aptitudes: Su grado de influencia en las ventas personales y en el éxito profesional.* MEXICO D.F.: daena international.

Secretaría de Relaciones Exteriores, S. J. (10 de abril de 2014). *taller sobre legislacion en materia de ciberdelincuencia en america latina* . Obtenido de Legislación en materia de Ciberdelincuencia : https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/2014/Memoria%20Taller%20Ciberdelito.pdf

Sevilla, D. C. (2011). la competitividad organizacional. *universidad del valle*, 11-13.

Social, C. N. (2011). *documento CONPES 3701.* BOGOTA: GOBIERNO NACIONAL.

Solorio, E. (2011). *Historia de la Cibernética, Computación y El Origen del Lenguaje Pascal.* Buenos Aires : CCH Sur.

Symantec. (26 de 01 de 2016). *Glosario de Seguridad 101*. Obtenido de Symantec. Confianza en un mundo Conectado: https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad

TIC. (12 de agosto de 2012). *Pedro José Cabrera Cabrera (Director).* Obtenido de Nuevas Tecnologías y exclusión social:

http://www.ohchr.org/Documents/Issues/CulturalRights/ConsultationEnjoyBenefits/UNESCONUEVAS_TECNOLOGIASyExclusionsocial.pdf

Torres, R. (2010). *METODOLOGIA DE ANALISIS DE RIESGO DE LA EMPRESA LA.* San Salvador : Universdidad Tecnologica del Salvador .

Vasco, U. d. (23 de marzo de 2008). *La teoría de sistemas de Niklas Luhmann*. Obtenido de La teoría de sistemas de Niklas Luhmann: http://www.uma.es/contrastes/pdfs/015/contrastesxv-16.pdf