PANORAMA ACTUAL DE LA SEGURIDAD INFORMÁTICA O DE LA CIBERSEGURIDAD, A NIVEL DEL PAÍS Y LAS TENDENCIAS ACTUALES Y FUTURA A NIVEL GLOBAL

ING. HERNANDO ARBEY ROBLES PUENTES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIAS E INGENIERIAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CCAV NEIVA
2018

PANORAMA ACTUAL DE LA SEGURIDAD INFORMÁTICA O DE LA CIBERSEGURIDAD, A NIVEL DEL PAÍS Y LAS TENDENCIAS ACTUALES Y FUTURA A NIVEL GLOBAL

ING. HERNANDO ARBEY ROBLES PUENTES

Monografía como opción de grado para optar el título de especialista en seguridad informática

Director de proyecto:

Ing. Juan José Cruz Garzón

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIAS E INGENIERIAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CCAV NEIVA

2018

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

_____

Neiva, 27-11-2018

DEDICATORIA

Dedico este trabajo a Dios todo poderoso que me ha iluminado el camino para llegar a este punto, a mi madre que desde el cielo también lo hace, a mi familia por el tiempo que he dejado de dedicarles, además de su gran apoyo para culminar esta etapa de mi vida.

AGRADECIMIENTOS

A mi director de proyecto de grado el Ingeniero Juan José Cruz Garzón, por permitirme que pudiera aplicar el conocimiento adquirido durante lapso de tiempo de mis estudios.

A los tutores del CCAV Neiva, que me brindaron su gran apoyo durante la formación académica de mi carrera Pos gradual, en especial al Ingeniero Pedro Torres Silva.

A la Universidad por brindarme la oportunidad de terminar mi ciclo de Posgrado de manera virtual.

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ILUSTRACIONES

Pág.

RESUMEN

Apenas hace unos pocos años, se ha iniciado la cultura de la seguridad informática, las organizaciones antes del año 2000 invertían mucho más en café y bebidas que en seguridad. Las tecnologías emergentes en el presente siglo, han superado cualquier pronóstico de penetración en todos los ámbitos tanto sociales, culturales, económicos y políticos y se han incorporado de una manera general a la vida de los países. Y con ello, han proliferado cualquier cantidad de ataques a la información de Gobiernos, de empresas y de personas. Lo que ha influenciado que muchos gobiernos, agencias multilaterales y empresas hayan tomado partido por la seguridad informática.

Frente a este hecho, ampliamente reconocido, los estados y las políticas gubernamentales han estado un paso atrás. En Colombia, solamente en el 2016, se produce la modificación al CONPES 3701/11, documento integral sobre seguridad digital y es a través del CONPES 3854, y en uno de sus apartes expresa:

> “El enfoque de la política de ciberseguridad y ciberdefensa, hasta el momento, se ha concentrado en contrarrestar el incremento de las amenazas cibernéticas bajo los objetivos de (i) defensa del país; y (ii) lucha contra el cibercrímen. Si bien esta política ha posicionado a Colombia como una de los líderes en la materia a nivel regional, ha dejado de lado la gestión del riesgo en el entorno digital.
>
> Enfoque esencial en un contexto en el que el incremento en el uso de las TIC para realizar actividades económicas y sociales, ha traído consigo nuevas y más sofisticadas formas de afectar el desarrollo normal de estas en el entorno digital. Hecho que demanda una mayor planificación, prevención, y atención por parte de los países.”

La propuesta gubernamental es que para el año 2020 este la política implementada. Lo cual muestra, un periodo de emergencia, cuando no todos los actores están comprometidos con el establecimiento de lineamientos sobre la ciberseguridad. A partir de este escenario, es importante realizar un estudio que determine un panorama mucho más profundo en la seguridad informática del país y comparado con lo que se ha desarrollado en otros países.

Palabras Claves: Seguridad Informática, seguridad de la información, infraestructura crítica, Amenaza informática, Ciberespacio, Ciberdefensa, Ciberseguridad

INTRODUCCIÓN

Hoy es irreversible el proceso de convergencia de la seguridad integral e integrada, cuando los países han incorporado las tecnologías de la información y comunicación en todos sus ámbitos. Cada día será mucho más complejo su gobernanza y su gestión, especialmente en la aplicación a las infraestructuras críticas, por ejemplo, energía, movilidad, etc., lo que obliga tratar los aspectos importantes desde una nueva perspectiva.

En este contexto, es impactante comprobar la complejidad de los desafíos actuales para la defensa y seguridad del siglo XXI, desde las graves repercusiones del cambio climático, el control de los sistemas financieros y de generación de riqueza hasta la evolución del terrorismo y delincuencia trasnacional, que están haciendo muy difusa la posibilidad de tener una base de estudio más clara y diferenciada de los conceptos asociados a la ciberseguridad.

Hoy la actividad empresarial está basada más que nunca en la tecnología, lo que conlleva la proliferación de plataformas y sistemas de los que se depende para realizar las actividades eficazmente y garantizar el funcionamiento de todas las infraestructuras críticas.

Se está, ante una nueva generación de amenazas sofisticadas como señala el hecho de que, por ejemplo, ahora, los cibercriminales disfrutan de un acceso superior: los virus y ataques son más sofisticados y explotan las vulnerabilidades con la intención explícita de apoderarse de datos valiosos y porque no, del control de los grandes sistemas.

Así, según el nivel de consecuencias en la infraestructura atacada y su grado de sofisticación y determinación, los requisitos de seguridad de TI de cualquier

empresa normal hoy constituyen todo un nuevo reto. El punto de partida de muchos de los ataques lanzados hoy en día consiste en explotar las vulnerabilidades de las aplicaciones de uso común.

Cuanto más complejas sean las tecnologías de seguridad y más tiempo tomen en aplicarse los cambios, mayor será el coste de la seguridad y menor la eficacia y rentabilidad de la inversión.

1. TÍTULO

Panorama actual de la seguridad informática o de la ciberseguridad, a nivel del país y las tendencias actuales y futura a nivel global

2. DEFINICIÓN DEL PROBLEMA

2.1. ANTECEDENTES DEL PROBLEMA

El reto que hoy tienen los estado y gobiernos está en poder desarrollar doctrinas, métodos y órganos que sean capaces de reacción de forma predictiva y porque no, proactiva a los ataques de la delincuencia globalizada, tal como lo plantea el Coordinador del programa Prospint[1] de la Secretaría de Estado de Seguridad, el ingeniero Andrés Montero en su documento de prospectiva de seguridad. Y para fundamentar el análisis se ha tomado, del mencionado texto lo siguiente:

> "El terrorismo y la delincuencia organizada global no sólo han retado las tradicionales concepciones de seguridad interior y exterior, sino que están poniendo de manifiesto que la seguridad reactiva o que la seguridad desgajada de la inteligencia son respuestas obsoletas de los Estados ante las amenazas. El desarrollo de doctrina, métodos y órganos para la inteligencia prospectiva de seguridad se presenta como una opción estructural para proporcionar a las instituciones de seguridad capacidades de respuesta inteligentes, preventivas y proactivas ante las nuevas amenazas.
>
> La seguridad pública es un concepto no reducible a la respuesta policial, sino un pilar horizontal de la libertad ciudadana que debe atender a todos los elementos que contribuyen a generar vulnerabilidades ante las amenazas, a desencadenarlas y a mantenerlas en el tejido social. La propuesta para ofrecer una respuesta funcional, eficaz y eficiente, es que los poderes públicos adopten enfoques de seguridad inteligentes basados en el

[1] Prospint es un programa de la Secretaría de Estado de Seguridad del Ministerio del Interior español

> conocimiento comprensivo de las amenazas. Ese conocimiento parte de análisis descriptivos exhaustivos de los fenómenos, para después adentrarse en explicar sus causalidades. La inteligencia basada en el conocimiento es el sustrato a partir del cual las instituciones de seguridad estarán en condiciones de abordar estudios prospectivos que sirvan de apoyo para la toma de decisiones hacia una seguridad preventiva, que reduzca los riesgos manejando sus incertidumbres."

Estos mismos conceptos de la delincuencia global y de los procesos reactivos de los agentes del estado para ejercer control y/o de las organizaciones cuando se habla de seguridad informática, son los que nos lleva a un análisis de la situación actual y presentar una visión prospectiva de la seguridad informática en el país.

Luego lo que implica, como se dice en los reglones anteriores, hoy se requiere de una respuesta funcional, eficaz y eficiente, sin vulnerar la libertad ciudadana. Luego requerimos de verdaderos análisis de los fenómenos asociados a los ataques cibernéticos.

2.2. FORMULACION DEL PROBLEMA

¿Cuál es el panorama actual de la seguridad informática o de la ciberseguridad, a nivel del país y las tendencias actuales y futuras a nivel global?

2.3. DESCRIPCIÓN DEL PROBLEMA

Es de común conocimiento que cualquier equipo informático que esté conectado a una red, su seguridad ya no será en el 100%. En especial cuando accedemos a Internet, al ser esta una red universal. Pero, este es una sola causa, el otro elemento

importante, es el acceso mismo a los equipos, a los dispositivos de interworking de una organización. Luego, podemos reconocer que dos riesgos sustanciales son la conectividad a las redes, en especial a Internet y la otra, desde al acceso físico.

Se plantea como el rompecabezas de la seguridad informática en el mundo. Desde la defensa de los equipos hasta el software y allí la información. Es claro que la seguridad se centra en tres elementos: Integridad, confidencialidad y disponibilidad de la información, y de estos conceptos se desprenden todos los elementos que constituyen ese rompecabezas. Se trazan las políticas globales, de los estados o públicas y de las organizaciones. Estas políticas más conocidas como normas de gestión, para el caso de Colombia, desde el Instituto Colombiano de Normas Técnicas y Certificación – ICONTEC, en el año 2006, publico la NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001. TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI).

Ahora, se debe conocer que tanto ha sucedido en el país desde la promulgación de esta norma. Como se está desarrollando en las entidades públicas y/o territoriales. Y su sistema de gestión de la seguridad de la información (SGSI). Y un país, como el nuestro, que está a las puertas de la adhesión como miembro de la *Organización para la Cooperación y el Desarrollo Económicos* (*OCDE*), en el proceso que se ha adelantado, para el año 2017, trabajaron en la evaluación del impacto del gobierno digital en Colombia.

Asimismo, no se pueden desconocer otras políticas públicas encaminadas al manejo de la información, como Gobierno en línea, donde uno de sus ejes temáticos es la **Seguridad y privacidad de la información que** busca guardar los datos de los ciudadanos como un tesoro, garantizando la seguridad de la información.

Luego el País, tiene legislación al respecto, que debe ser revisada.

3. JUSTIFICACIÓN

Con las tecnologías emergentes, en especial las que ya están incorporando inteligencia artificial y otras, aún más sagaces, dispositivos de seguimiento y/o de comportamiento de los consumidores se hace necesario abordar el tema de la seguridad informática, no solo desde los elementos y políticas de protección de la información sino en el seguimiento a los procesos y/o compromisos del Estado, para alcanzar niveles de seguridad acorde a los estándares internacionales.

Desde la academia, se ha escrito lo suficiente en los modelos técnicos de seguridad (Hardware, software, políticas de acceso, políticas de gobernanza TI), pero hace falta, ir más allá. Donde ha trascendido en la cultura ciudadana, el ejercicio de su compromiso con la seguridad.

El nivel de incremento de los delitos informáticos y los asociados a las TIC y es cada día más preocupante. Cuando se lee sobre las causas de estos delitos, es el ciudadano quien ha permitido la ocurrencia por el mal manejo de su información. Pero no por ello, se debe hacer caso omiso a este problema mundial.

Se expone la seguridad al compartir información que para el atacante es valiosa, en las redes sociales. Todo esto demuestra que, en el país, es un tema que aún no trasciende al ciudadano común y la gran mayoría de las empresas tanto públicas como privadas han avanzado en la incorporación de las TIC en todos sus procesos, especialmente en el manejo de datos abiertos.

No es un panorama claro, por ello, el indagar, analizar, y describir la situación actual nos ofrecerá un apoyo sustancial para el mejoramiento de las políticas de seguridad de la información y de los sistemas de gestión de la seguridad informática.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Describir el panorama actual de la seguridad informática o de la ciberseguridad, a nivel del país y las tendencias actuales y futura a nivel global.

4.2. ESPECÍFICOS

1. Realizar indagación sobre cada una de las normas que conforman la política pública del país sobre la seguridad de la información.

2. Realizar un contraste de las políticas públicas y la aplicación real en el País, en sus entidades públicas y/o entes territoriales.

3. Describir el panorama actual de la seguridad informática del país.

4. Describir las tendencias actuales y futuras de la seguridad de la información o de la ciberseguridad.

5. MARCO REFERENCIAL

5.1. MARCO TEÓRICO

Toda organización debe estar a la vanguardia de los procesos de cambio donde disponer de información continua, confiable y en tiempo, constituye una ventaja fundamental donde tener información es tener poder donde la información se reconoce como, crítica, indispensable para garantizar la continuidad operativa de la organización. Es un activo corporativo que tiene valor en sí mismo que debe ser conocida por las personas que necesitan los datos. Siendo coherente con el concepto de la norma ISO/IEC 17799 (2005), y coherente con:

> "Esto es especialmente importante en el ambiente comercial cada vez más interconectado. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades"

Asimismo, en la misma línea de la OCDE (2004) en su documento de Guías de la OCDE para la seguridad de los sistemas de información y redes. Específicamente cuando advierten:

> "Como resultado de la creciente conectividad, los sistemas de información y las redes son más vulnerables ya que están expuestos a un número creciente, así como un rango de variedad mayor de amenazas y vulnerabilidades. Esto hace que surjan nuevos retos que deben abordarse en el tema de seguridad. Por estas razones, estas guías aplican para todos los participantes de la nueva sociedad de la información y sugieren la necesidad de tener una mayor consciencia y entendimiento de los aspectos de seguridad, así como de desarrollar una "cultura de seguridad".

Para ello, se deben fundamentar en nuevo (9) principios de actuación:

- Concientización
- Responsabilidad
- Respuesta
- Ética
- Democracia
- Evaluación del riesgo
- Diseño e implementación de seguridad.
- Administración de la Seguridad.
- Reevaluación

El Sistemas de Información debe ser el de preservar la Confidencialidad. Asegurándose que la información es accesible sólo a las personas autorizadas proteger la información contra accesos o divulgación no autorizados la falta de confidencialidad puede darse por indiscreciones voluntarias e involuntarias en cualquier tipo de soporte y su no preservación puede tener las siguientes consecuencias:

- Responsabilidad civil o administrativa
- Pérdidas cualitativas en distintos campos
- Deontología
- Credibilidad
- Prestigio
- Imagen
- Pérdidas de fondos patrimoniales:
- Datos o programas no recuperables
- Información confidencial
- Pérdidas de explotación

- Reducción de margen por falta de resultados o gastos suplementarios

Bajo los principios anteriores, se revisaron los conceptos necesarios para el desarrollo de este trabajo en cuatro elementos fundamentales: Ciberdefensa: Situación actual, Ciberseguridad, Estrategia Nacional de ciberseguridad y una comparación de los diferentes modelos.

A. Ciberdefensa: Situación Actual

Como ya se ha descrito, cuanto mayor es el índice de desarrollo de una sociedad, mayor dependencia se tiene de los sistemas de información y de las comunicaciones. Las empresas, la sociedad, el gobierno y la defensa nacional dependen del funcionamiento de las tecnologías de la información y comunicaciones (TICs) y de la operación de las Infraestructuras Críticas de Información (ICIs). Cualquier intrusión, manipulación, sabotaje o interrupción de dichos sistemas y de las ICIs pueden llegar a ser sufridos por millones de personas.

Para el ciberespacio no hay frontera mientras que para los conflictos tradicionales existen fronteras y límites. Una de las principales características de este tipo de fenómeno, el ataque, no es necesario desplazarse, moverse o tener que pasar una frontera. Sin fronteras geográficas, anónimo, asimétrico y puede ser considerado fácilmente clandestino. Esto es, es un ambiente único.

La ciberdefensa es la aplicación de medidas de seguridad para proteger las infraestructuras de los sistemas de información y comunicaciones frente a los ciberataques (Acosta et al., 2009).

Hoy, es muy fácil encontrar en internet herramientas de ethical hacking para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas. Pero, su uso no está controlado y teniendo en cuenta que el grado de conocimiento que necesita un atacante para realizar una agresión a los sistemas de información ha decrecido

a lo largo del tiempo, debido al aumento de la calidad, cantidad y disponibilidad de herramientas ofensivas. También, existen herramientas de informática forense y de seguridad informática, entre otras, que son utilizadas con mala intención. Ciberdefensa debe ser considerada como un riesgo al que es preciso hacer frente para mejorar la seguridad nacional. Este es un escenario de nuevos riesgos.

Un factor importante es la falta de conciencia en seguridad de algunas partes de la sociedad, lo que dificulta tomar medidas eficaces y poder coordinarlas. Asimismo, que muchos de los objetivos propensos para ser atacados no solamente están en manos del Gobierno sino también de empresas privadas. Esto hace que defenderse sea mucho más complejo. Aún más, cuando las empresas privadas, dependen en gran medida de las acciones que toman éstas para asegurar sus sistemas, lo que implica asumir los costos que en ocasiones no se están dispuestos a asumir, y generan unos riesgos muy significativos.

B. Ciberseguridad

De acuerdo al grupo de trabajo bilateral rusoestadounidense del EastWest Institute (EWI) y la Universidad de Moscú elaboro en el 2011 un marco de terminología internacional. Donde definen la Ciberseguridad como "una propiedad del ciberespacio, que tiene la capacidad de resistir las amenazas intencionales y no intencionales, responder y recuperarse" [Rauscher y Yashenko, 2011, página 31].

Este concepto de la Ciberseguridad se refiere generalmente a la capacidad de controlar el acceso a las redes, sistemas de información y todo tipo de recursos de información. Sin embargo, donde los controles de Ciberseguridad están ausentes, incompletos, o mal diseñados, el ciberespacio es considerado como tierra de nadie.

Prevenir, detectar, responder y recuperarse se señalan actualmente como los objetivos de la Ciberseguridad, pero tradicionalmente el objetivo principal fue prevenir que se concrete un ataque exitoso, esto es, sistemas reactivos. Sin

embargo, todos los profesionales de seguridad son conscientes de que simplemente no es posible evitar todos los ataques y que debe existir una planificación y preparación que incluya métodos para detectar ataques en progreso, preferentemente antes de que causen daño, como ejemplo los HoneyPot. Luego la expectativa más positiva en Ciberseguridad, es la de tener la capacidad de responder, y además también recuperar o corregir. Y, en cualquier caso, serán las lecciones aprendidas respecto de las respuestas a incidentes y la recuperación, las que alimentarán la estructuración y planificación para la prevención.

Por ello, ya sea un usuario individual de internet, un pequeño negocio, una institución, entidades públicas o empresas privadas, deben construir e implementar su propia política para mantener la seguridad en el ciberespacio y estas deben estar directamente correlacionadas entre si y poder responder a una estrategia de nivel superior con una misión y un propósito como nación.

Es claro que correlacionar políticas y estrategias de ciberseguridad no es una tarea fácil, y no se basa solo en la aplicación de la ley y del establecimiento de una política pública sin su respectiva socialización e integración a todos los niveles, la gestión y la tecnología, requiere una forma consensuada y armoniosa de actuar y resaltar la necesidad de innovación.

C. Estrategia Nacional de Ciberseguridad

Leyva[2] (2015) plantea: “Como se mencionó anteriormente a medida que la sociedad se vuelve más dependiente de las TICs, la protección y la disponibilidad de los servicios críticos se vuelven un tema de interés nacional. Los incidentes que causan la interrupción de las infraestructuras críticas y de los servicios podrían causar importantes impactos negativos en la sociedad y en la economía. Asegurar el

[2] Leiva E. 2015. *Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local* Revista Latinoamericana de Ingeniería de Software, 3(4): 161-176, ISSN 2314-2642

ciberespacio se ha convertido en uno de los retos más importantes de la actualidad y es considerado como una cuestión nacional a nivel estratégico que afecta a todos los niveles de la sociedad.

Por lo tanto, una Estrategia Nacional de Ciberseguridad se define como "un plan de acción nacional sobre la base de una visión nacional para lograr un conjunto de objetivos que contribuyan a la seguridad del ciberespacio" [Luiijf et al.,2013]. Se encuentra a un alto nivel en la pirámide organizacional de una nación, y establece una serie de objetivos nacionales y prioridades que deben alcanzarse en un plazo determinado. Como tal, proporciona un marco estratégico para la implementación de un Sistema de Ciberseguridad Nacional, que se entiende como un conjunto de órganos, organismos y procedimientos que permiten la dirección, control y gestión de la Ciberseguridad."

En Colombia, como estrategia de Ciberseguridad y como política pública se han desarrollado dos documentos llamados CONPES, el primero del año 2011 y el segundo del año 2016. Y que no corresponden a lo mencionado por Leyva (2015), que debe ser sobre una base de visión nacional que permitan el alcance de los objetivos que realmente permitan obtener un sistema de seguridad del ciberespacio. Aun cuando, está en la cúspide de la pirámide organizacional de la Nación, no son claros y mucho menos tienen temporalidad para su cumplimiento.

Se revisó el documento CONPES 3701 de 2011, donde se establecen los primeros elementos de seguridad, así:

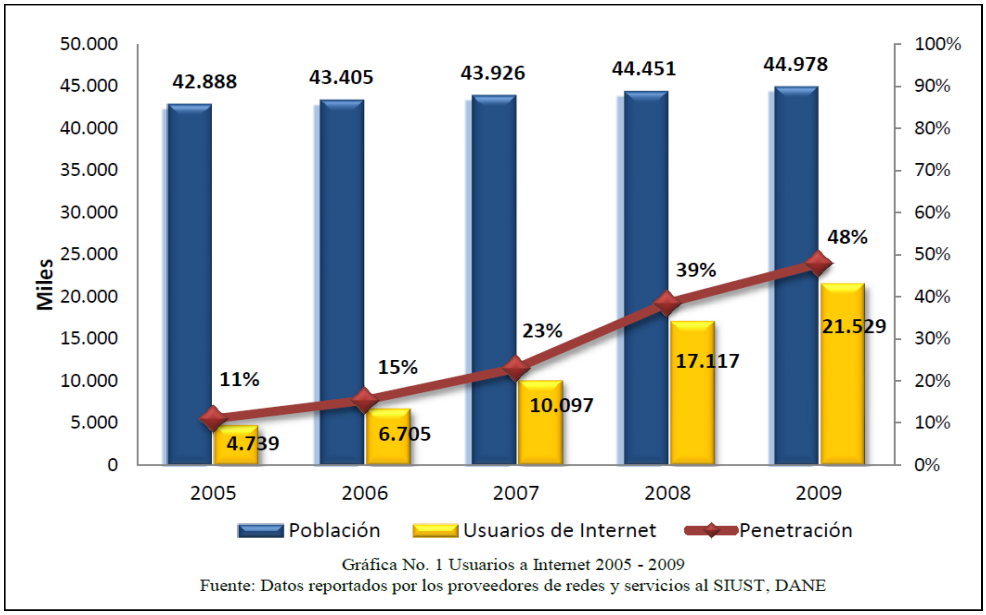
> "Este documento busca generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. Adicionalmente, recoge los antecedentes

nacionales e internacionales, así como la normatividad del país en torno al tema."

Donde definen la ciberseguridad, como: "Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética. "Y, la ciberdefensa, como la Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional.

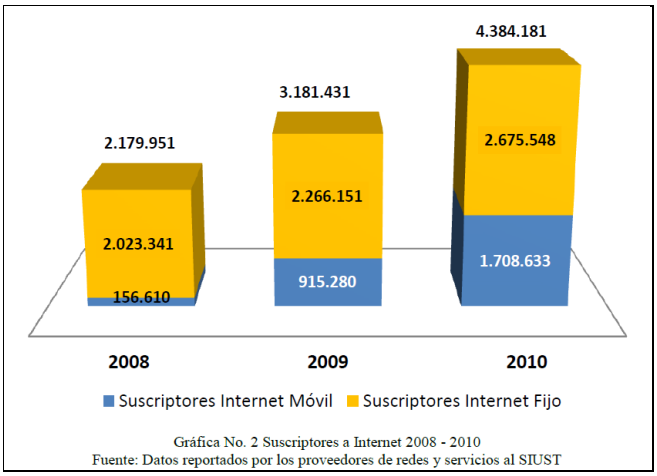
En la descripción del problema en el documento CONPES, se plantean varias situaciones acaecidas en los años anteriores, en especial los casos de Estonia (2007), y el otro, el desmantelamiento de la red de computadores "zombies" conocida como "BotNet Mariposa." Donde Colombia, ocupo el quinto lugar de los países más afectados por este fenómeno. Asimismo, en el documento CONPES, se reconoce el crecimiento casi exponencial. Con incrementos superiores al 101% entro los años 2008 a 2010.

Ilustración 1 . Crecimiento de los usuarios de Internet en Colombia.



Fuente: CONPES 3701 de 2011, página 8.

Ilustración 2. Crecimiento de suscripciones de Internet móvil e Internet Fijo.



Fuente: Documento CONPES 3701/11, página 8.

Donde uno de los riesgos más importantes que el cambio de cultura de la población colombiana, en el uso de Internet para las transacciones financieras. Para el año 2011, alcanzaba el 30% de las operaciones bancarias. En el mismo documento se comenta:

> "En relación con seguridad cibernética, Colombia también ha sido objeto de ataques. Un caso a resaltar fue el ocurrido durante el primer semestre de 2011, cuando el grupo "hacktivista" autodenominado Anonymous atacó a los portales de la Presidencia de la República, el Senado de la República, Gobierno en Línea y de los Ministerios del Interior y Justicia, Cultura y Defensa, dejando fuera de servicio sus páginas web por varias horas. Este ataque se dio en protesta al Proyecto de Ley "por el cual se regula la responsabilidad por las infracciones al derecho de autor y los derechos conexos en Internet". Este grupo ha atacado indistintamente entidades públicas y privadas, entre las que se cuentan PayPal, el banco suizo *Post Finance*, MasterCard, Visa y páginas web del gobierno suizo."

Esto demuestra que solamente en el 2011, el gobierno advierte de los peligros sobre la seguridad de la información. Y obliga en el año 2016, a redefinir y profundizar sobre los temas de seguridad de la información y la seguridad informática, donde se posesionan los dos conceptos anteriores de Ciberseguridad y Ciberdefensa.

En el resumen ejecutivo del documento CONPES 3854 de 2016, dice:

> “El creciente uso del entorno digital en Colombia para desarrollar actividades económicas y sociales, acarrea incertidumbres y riesgos inherentes de seguridad digital que deben ser gestionados permanentemente. No hacerlo, puede resultar en la materialización de amenazas o ataques cibernéticos, generando efectos no deseados de tipo económico o social para el país, y afectando la integridad de los ciudadanos en este entorno.
>
> El enfoque de la política de ciberseguridad y ciberdefensa, hasta el momento, se ha concentrado en contrarrestar el incremento de las amenazas cibernéticas bajo los objetivos de (i) defensa del país; y (ii) lucha contra el cibercrímen. Si bien esta política ha posicionado a Colombia como una de los líderes en la materia a nivel regional, ha dejado de lado la gestión del riesgo en el entorno digital. Enfoque esencial en un contexto en el que el incremento en el uso de las TIC para realizar actividades económicas y sociales, ha traído consigo nuevas y más sofisticadas formas de afectar el desarrollo normal de estas en el entorno digital. Hecho que demanda una mayor planificación, prevención, y atención por parte de los países.
>
> Es precisamente por esto que la política nacional de seguridad digital, objeto de este documento, cambia el enfoque tradicional al incluir la gestión de riesgo como uno de los elementos más importantes para abordar la seguridad digital. Esto lo hace bajo cuatro principios fundamentales y cinco dimensiones estratégicas, que rigen el desarrollo de esta política. De los primeros destaca

que la política nacional de seguridad digital debe involucrar activamente a todas las partes interesadas, y asegurar una responsabilidad compartida entre las mismas. Principios que se reflejan en las dimensiones en las que esta política actuará, las cuales determinan las estrategias para alcanzar su objetivo principal: fortalecer las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital. Para lograrlo, se implementarán acciones en torno a cinco ejes de trabajo.

En primer lugar, se establecerá un marco institucional claro en torno a la seguridad digital. Para esto, se crearán las máximas instancias de coordinación y orientación superior en torno a la seguridad digital en el gobierno, y se establecerán figuras de enlace sectorial en todas las entidades de la rama ejecutiva a nivel nacional. En segundo lugar, se implantarán las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital, mediante mecanismos de participación activa y permanente, la adecuación del marco legal y regulatorio de la materia y la capacitación para comportamientos responsables en el entorno digital. Como tercera medida, se fortalecerá la defensa y seguridad nacional en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos. Por último, se generarán mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico.

Para poner en marcha esta política, se ha construido un plan de acción que se ejecutará durante los años 2016 a 2019 con una inversión total de 85.070 millones de pesos. Las principales entidades ejecutoras de esta política son el Ministerio de Tecnologías de la Información y las Comunicaciones, el

Ministerio de Defensa Nacional, la Dirección Nacional de Inteligencia y el Departamento Nacional de Planeación.

Se estima que la implementación de la política nacional de seguridad digital al año 2020 podría impactar positivamente la economía de Colombia, generándose durante los años 2016 a 2020 alrededor de 307.000 empleos y un crecimiento aproximado de 0,1% en la tasa promedio de variación anual del Producto Interno Bruto (PIB), sin generar presiones inflacionarias."

Se plantea, que este documento que genera los recursos del estado, son de exclusividad para:

- Defensa del país
- Lucha contra el cibercrímen

Y son responsables de su ejecución los ministerios de las TIC y el de defensa, con el apoyo del Departamento de planeación nacional y la dirección nacional de inteligencia.

Esto es, dicho de otra forma, el estado se defiende con sus propios recursos. Y que ocurre, con las empresas y aún más importante, con los ciudadanos.

D. Comparación de Estrategias Nacionales de Ciberseguridad

Colombia como miembro de la OEA, suscribe en el 2004 la Estrategia Interamericana Integral de Ciberseguridad. Conforme fue evolucionando el panorama de las amenazas, los esfuerzos de los gobiernos también lo hicieron, aprobaron una declaración sobre el "Fortalecimiento de la Ciberseguridad en las Américas" en marzo de 2012.

Se toma el cuadro elaborado por Leyva (2015, página 169) donde se observa que en la región los dos países que mayor han avanzado en la construcción de una estrategia nacional son Brasil y Colombia.

Tabla 1. Cuadro comparativo de las políticas de ciberseguridad en la Región.

	BLOQUE GEOPOLÍTICO	OEA			
	PAÍS	COL	BRA	CHILE	ARG
PROTEGE	Infraestructuras criticas	X	X	X	X
	Economía		X		
	Seguridad Nacional		X		
	Bienestar Social	X	X		
ENFOQUE	Concientización	X	X	X	
	Conocimiento		X		
	Educación	X	X	X	
	Capacidades cibernéticas militares	X			
SECTOR PUBLICO	Liderazgo/coordinación	X	X	X	X
	Marco jurídico	X			X
SECTOR PRIVADO	Participación en la estrategia	X	X	X	
COOPERACIÓN INTERNACIONAL	Cooperación en su grupo	X	X	X	X
	Cooperación con otros países	X	X	X	X

Fuente: Leiva E. 2015. Estrategias Nacionales de Ciberseguridad, Pagina 169.

Es claro que para los cinco elementos fundamentales: Protege, enfoque, Sector público, Sector privado y Cooperación Internacional, Colombia cumple de buena manera, ahora es saber si son funcionales las políticas trazadas y si verdaderamente van en la dirección correcta.

5.2. MARCO CONCEPTUAL

En una estructura, o en el dominio de control, se puede observar que existen cuatro (4) elementos de seguridad que están contenidos en las Normas ISO:

1. Seguridad organizativa
    a. Políticas de seguridad
    b. Aspectos organizativos para la seguridad
    c. Clasificación y control de activos
    d. Seguridad ligada al personal
    e. Gestión de continuidad del negocio

2. Seguridad lógica
    a. Control de accesos

    “Como resultado de la creciente conectividad, los sistemas de información y las redes son más vulnerables ya que están expuestos a un número creciente, así como un rango de variedad mayor de amenazas y vulnerabilidades. Esto hace que surjan nuevos retos que deben abordarse en el tema de seguridad. Por estas razones, estas guías aplican para todos los participantes de la nueva sociedad de la información y sugieren la necesidad de tener una mayor consciencia y entendimiento de los aspectos de seguridad, así como de desarrollar una “cultura de seguridad”.

    a. Desarrollo y mantenimiento de sistemas
    b. Gestión de comunicaciones y operaciones

3. Seguridad física
    a. Seguridad física y del entorno

4. Seguridad legal
    a. Conformidad

Con una estructura desde lo táctico, lo estratégico y lo operacional. De acuerdo a lo expuesto por Antonio Villalón Huerta, en su presentación: “Códigos de buenas prácticas de seguridad. UNE/ISO/IEC 17799” Que encierra en esta triada y debe mantenerse con el fin de verdaderamente garantizar la seguridad de la información.

Es por ello, muy importante, trabajar e indagar como está el país, como está la construcción de una cultura de protección de la información, cuando la exponemos en programas de gobierno en línea, datos abiertos, e-gobierno, etc.

No se considera necesario hacer todo en recorrido teórico sobre la seguridad, solamente las pautas por las cuales se podrá desarrollar este trabajo, en especial en el reconocimiento de las normas internacionales, de los compromisos de Colombia como país y de la dedicación de algunas empresas en el tema de la protección de datos y por ende de los ciudadanos. Pero sí que se debe tener claro que el tema de seguridad es reflexionar y analizar sobre los retos a los que cada uno de los ciudadanos del mundo, con ligeras o significativas diferencias, pero, todos dentro del marco especial que representa la globalización para este sector, son expuestos.

Las cuestiones económicas, con atención a la coyuntura internacional y las implicaciones en el ámbito energético, la innovación digital, así como los conflictos regionales, el terrorismo y los flujos migratorios, son conceptos que ya manejamos casi de forma global.

De acuerdo a lo expresado por el Consultor internacional, Manuel Sánchez Gómez-Merelo[3]:

> “El escenario internacional actual, ya sea a escala mundial o a nivel regional o local, resulta en muchos casos inquietante para nuestra seguridad, para la recuperación del bienestar perdido durante la crisis, e incluso para la defensa de algunos de los valores democráticos y liberales más importantes que compartimos una gran mayoría de países.
>
> Sin embargo, no nos vamos a sumar a ningún tipo de pesimismo, ya que, aún con la necesidad de estar preparados para escenarios de alto riesgo, el panorama internacional sigue ofreciendo muchas oportunidades que debemos abordar de forma proactiva.
>
> Esta contribución se debe enfocar positivamente, pese a que las experiencias y percepciones de inseguridad se articulan en formas que no son ni obvias ni sencillas. Baste pensar que el riesgo de mayor impacto para la seguridad global lo proporcionan los efectos derivados del cambio climático, por delante de otros tales como el terrorismo o el crimen organizado.
>
> Es un hecho que el propio metabolismo de la globalización produce miedo e inseguridad que invaden amplias zonas del planeta, y nuestro mayor reto está en lograr una adecuada gobernanza, una inteligente gestión de los riesgos y de los conflictos.
>
> Las estrategias tradicionales de seguridad, fracasadas por el mal análisis de los riesgos y los conflictos que las motivan, terminan por formar parte del problema en lugar de la solución.

[3] MANUEL SANCHEZ GÓMEZ-MERELO, Blog sobre convergencia y tecnología de Tendencias21 https://www.tendencias21.net/seguridad/

En este sentido, hemos de acometer una serie de reflexiones sobre que estos riesgos pues los conflictos no pueden ya seguir siendo considerados como "efectos colaterales o secundarios" del proceso de modernización de la sociedad industrial y de la información, sino que, por el contrario, constituyen un componente más de este proceso.

¿Qué ha pasado en 2017?

Acabamos de pasar un año 2017 plagado de acontecimientos en los que la inseguridad nos ha hecho percibir su presencia en territorios y temas que superan lo conocido hasta ahora en la sociedad del bienestar. El terrorismo, los conflictos regionales y, especialmente, el creciente número de incidentes de ciberseguridad han tenido cierto protagonismo, ocupando en gran medida los titulares de los principales medios de comunicación. Hemos de reflexionar y procesar todo lo ocurrido y poner nuestra mirada sobre el año que comenzamos en el que, sin duda, se generarán interesantes discusiones sobre el panorama de amenazas y la gestión de los riesgos.

Algunos acontecimientos ocurridos en determinadas partes del mundo durante el año 2017 no auguran nada bueno, toda vez que los protagonistas de los conflictos internacionales se encuentran en proceso de nuevo posicionamiento, lo que nos obliga a analizar el balance de lo ocurrido en este año convulso, pero, sobre todo, a adelantar una hipótesis de los resultados de esa prospectiva, con algunas claves que deberían ayudar a afrontar mejor el panorama, tanto inmediato como más lejano.

¿Hacia dónde en 2018?

El año entrante hemos de enfrentarnos a una serie de desafíos diversos y significativos como: las tensiones geoestratégicas intensificadas por los

conflictos en curso; el incremento en la globalización del terrorismo yihadista; la inseguridad ciudadana derivada de las desigualdades sociales y el impacto del crimen organizado; el uso insostenible de los recursos naturales de nuestro planeta y el cambio climático.

De todos modos, y aunque estas realidades puedan representar un panorama ensombrecedor, no resulta tan temerario afrontar 2018 con ánimo positivo, dados los avances y expectativas a nivel global que se pueden ver, por ejemplo, en el recorrido de los acuerdos sobre cambio climático alcanzado en París, las nuevas sendas que alejan a Irán y Corea del Norte de la condición de amenaza nuclear, o en una posible cooperación internacional eficaz contra el terrorismo.

Pero, quizá sea la crisis de los refugiados, con sus diversas variables externas, donde esté uno de los principales retos y la UE se juegue su cohesión interior y su seguridad este nuevo año.

Por otro lado, también está el riesgo, con una notable probabilidad de que suceda, de un importante movimiento de flujos migratorios involuntarios a gran escala, afectando igualmente en gran medida al continente europeo, como consecuencia de los efectos del cambio climático, según indicaba ya The Global Risks Report 2016.

Por otra parte, las Ciberamenazas y los ataques informáticos llegaron para quedarse. Este año se prevé que los ataques continuarán expandiéndose tanto en volumen como en modalidades de enfoque. Sin embargo, aunque hemos de pensar que podrán evolucionar y diversificarse, hemos de insistir en la importancia de mantener un posicionamiento efectivo a favor de la ciberseguridad global, basado en el conocimiento del valor de la información,

complementándose además con la información y comprensión del panorama y el análisis de las amenazas.

Seguridad Mundial. Globalización de la seguridad

Con independencia de que el principal reto exterior que tenemos como país es conectarnos mejor con la integración europea dentro del objetivo de globalización de la seguridad, hemos de tener en cuenta que lo urgente, lo inmediato y lo importante en esta materia son tareas de difícil discernimiento y actualmente, las prioridades políticas se centran en la lucha contra el terrorismo y el crimen organizado (pese a no ser el área de más graves consecuencias), a fin de ofrecer la mejor seguridad ciudadana en su más amplio espectro.

Si nos referimos a la lucha contra el terrorismo, este está evolucionando constantemente hacia formas nuevas y cada vez más peligrosas con la intención de evitar las medidas de seguridad que se implementan en cada momento.

En este sentido, el “Global Risks Report 2016” destaca aspectos como el drama de los refugiados o la amenaza terrorista indicando que el mundo se enfrenta a un auténtico cambio de paradigma sobre lo que significa la libre circulación de bienes, personas e ideas.

Por otra parte, aunque combatir el terrorismo yihadista ya era considerado como la primera prioridad a la que debería atender la política exterior, como en el caso de España, uno de los aspectos más inquietantes del terrorismo contemporáneo radica en su dimensión transnacional y en el vínculo de una parte significativa de su actividad con el Crimen Organizado Global, especialmente con el tráfico de armas y el narcotráfico.

No obstante, hay que tener igualmente en cuenta a lo que llamamos la seguridad "*glocal*" (global + local), ese bien público que se coproduce con la participación de la sociedad civil y la responsabilidad de los actores estatales y colaboraciones internacionales.

Por otro lado, y refiriéndonos al Crimen Organizado, este está impulsado principalmente por la desregulación y la globalización financiera, esa diferenciación entre actividad económica legal y criminal, dinero limpio y dinero sucio, en la que resulta cada vez más difícil una represión eficaz pues supondría, en gran medida, cuestionar los principios mismos que rigen el concepto de globalización. Por consiguiente, el crimen organizado global se acomoda perfectamente a la parcelación del poder existente, principalmente en el mundo liberal.

En cuanto a la Seguridad Ciudadana, concepto ampliamente difundido desde finales de la década de los 90, que marca un cambio radical con respecto a las políticas estatales o nacionales de seguridad al enfatizar la calidad de vida y la dignidad humana, está igualmente vinculado con otros conceptos tales como la libertad y los derechos universales.

Sin embargo, sobre lo anterior, mientras que inicialmente el debate sobre la seguridad ciudadana trataba la inseguridad como un problema social, en años recientes se podría decir que se ha venido transformando el concepto de seguridad, demostrándose que resulta de una problemática del desarrollo. Un ejemplo de ello se encuentra en el "Informe sobre el Desarrollo" del Banco Mundial que explícitamente argumenta que es crítico "aceptar los vínculos que existen entre la seguridad y los resultados del desarrollo".

Por otro lado, hay que tener en cuenta que el fenómeno social de la inseguridad ciudadana se ve agravado por la extraordinaria capacidad que han adquirido los medios de comunicación a la hora de difundir en tiempo real y amplificar a nivel mundial -y, por tanto, deslocalizándolos- los desastres y las violencias más extremas y aterrorizantes.

Pero también contribuye, decisivamente, a la extensión de esta auténtica epidemia social, la inexistencia de indicadores y análisis fiables de la dimensión y la evolución real de la inseguridad a las que se ven sometidos los datos disponibles sobre las actividades de los organismos policiales y judiciales donde ni siquiera está claro que la delincuencia esté aumentando por encima del crecimiento económico y de población o de la movilidad local y transnacional.

Y, en todo caso, convendría ubicar esta amenaza en el lugar que le corresponde, por su gravedad relativa, en el conjunto de inseguridades como: las víctimas en las carreteras, los accidentes laborales o la violencia doméstica y la catástrofe ecológica.

A modo de conclusiones, podemos decir que, en el mundo globalizado en el que vivimos, más allá de las consignas mediáticas y las prioridades políticas (terrorismo internacional, crimen organizado y seguridad ciudadana), debemos entender que la inseguridad globalizada nos obliga a fijar la atención en los temas fundamentales que más graves consecuencias provocan, tanto en pérdidas de bienes como en vidas humanas (las amenazas derivadas del cambio climático, flujos migratorios, desigualdad, pobreza, corrupción, explotación, estados fallidos o totalitarios, terrorismo institucional, etc.).”

Como es sabido, cuando hablamos de seguridad de la información nos referimos a un vasto campo con numerosas facetas: seguridad técnica (lógica según algunos), administrativa y organizativa, que abarca los aspectos de gestión, legal y física. Dejando al margen de nuestra reflexión la seguridad física (por su menor relevancia frente a las restantes citadas) comenzaremos nuestras especulaciones por la seguridad legal.

A partir del análisis anterior que nos abre una visión diferente donde el tema de seguridad no solamente es local sino trasnacional y que, en este escenario, proteger no solamente las personas sino también, la información. Esta correlación entre seguridad en general y seguridad de la información determina de gran manera la seguridad de las personas.

En los documentos revisemos la situación actual del País de acuerdo a la normatividad existente, en especial los documentos de donde se establecen las políticas públicas.

5.3. MARCO JURIDICO

Adoptó en el año 2011 una Estrategia Integral de Ciberseguridad y Ciberdefensa conocida como el “CONPES 3701”. 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.

- El **Comando Conjunto Cibernético** (CCOC): una unidad militar que responde a ataques contra los bienes militares de la nación.

- El **colCERT**: la entidad coordinadora a nivel nacional que supervisa todos los aspectos de la Ciberseguridad y la Ciberdefensa.

En cuanto a la cooperación y el intercambio de información entre el sector privado y las autoridades gubernamentales, existe una norma específica, el Decreto 1704 (2012), que establece los requisitos que deben cumplir los proveedores de redes y servicios de telecomunicaciones a fin de respaldar, de manera eficaz y oportuna el trabajo de las autoridades nacionales. Además, las autoridades nacionales procuraron forjar relaciones con entidades claves del sector privado con el objeto de incrementar aún más la cooperación y el intercambio de información.

La cooperación internacional ha sido sólida, puesto que las autoridades nacionales colaboraron, de modo directo, con otras naciones en la respuesta a ataques cibernéticos o delitos cibernéticos. Un ejemplo de esto fue la participación activa de las autoridades colombianas en una iniciativa multinacional, bajo el auspicio del Grupo de Trabajo Latinoamericano sobre Delitos Tecnológicos de INTERPOL, cuyo objeto era identificar y arrestar a los usuarios de foros online donde se intercambiaba y distribuía material sobre pedofilia. Entre los países que colaboraron, se encuentran Argentina, Brasil, Chile, Costa Rica, Ecuador, Uruguay, Venezuela y España.

En el año 2016, se expide el CONPES 3854 de 2016. Es un ajuste a las políticas del Gobierno en un intento por mejorar la ciberseguridad y la ciberdefensa. Asimismo, se acoge a la declaración sobre el “Fortalecimiento de la Ciberseguridad en las Américas” en marzo de 2012. Donde uno de sus compromisos está la de establecer una Comisión de alto nivel para que construya y fortalezca las políticas públicas.

6. ESQUEMA TEMÁTICO

6.1. CAPITULO I: Normas que conforman la política pública del país sobre la seguridad de la información

El tipo de investigación está centrado de una parte al análisis de la situación actual, donde de cierta manera, que el método de análisis consiste en la descomposición de un todo en sus elementos, de acuerdo a los objetivos específicos planteados. El método analítico consiste obliga a la separación de las partes para estudiarlas en forma individual.

Ya se ha mencionado en apartes anteriores de las tres normas que tiene el país frente a la Ciberseguridad. Dos (2) CONPES y un Decreto sobre los requisitos de los proveedores de redes y de servicios de telecomunicaciones. Además de la Ley 1341 de 2009 ("Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones"), El cual está orientado al tema de las interceptaciones y manejo de información exclusiva del sector Judicial y del uso del espectro.

Además de los Documentos CONPES, el trabajo se ha desarrollado en una revisión de otros documentos fundamentales como:

- Guías de la OCDE para la seguridad de los sistemas de información y redes. Hacia una cultura de seguridad.
- Test de penetración como apoyo a la evaluación de riesgos en seguridad de la información.
- Ciberseguridad, la protección de la información en un mundo digital.
- Estudio exploratorio prospectiva de la industria TI en Colombia, 2015

Realmente que se encuentra, Colombia tiene claridad en la necesidad de establecer las políticas sobre Ciberseguridad, pero en el desarrollo de las misma se evidencia un claro objetivo de reacción ante los ataques informáticos. Poco se observa, que existan líneas claras y objetivas centradas en políticas de educación, prevención y de participación activa de los diferentes actores.

No es profunda la decisión del estado para crear organismos intersectoriales que permitan desde los diferentes escenarios realizar y preparar a la comunidad en el uso racional de las tecnologías, así como, los mecanismos para el reporte de incidentes sobre potenciales ataques recibidos.

6.2. CAPITULO II: Contraste de las políticas públicas y la aplicación real en el País

Al hacer el contraste de las políticas públicas y la aplicación real en el País, en sus entidades públicas y/o entes territoriales, se encuentra aún mucho más lejos del escenario deseado.

Las autoridades regionales y municipales, salvo contadas excepciones (Antioquia, Medellín, Bucaramanga, Bogotá) son mínimos los avances en los temas de Ciberseguridad. Es así, como información tan fundamental como lo son, los temas financieros oficiales, no gozan de las mínimas normas de seguridad.

Otros sectores muy sensibles, como es el sector salud, no ha logrado la integración de plataformas y la causa fundamental está en la protección de la información que allí se intercambia.

Una de las políticas que integra el concepto de seguridad de la información es la llamada Gobierno en Línea. Creado con el Decreto 1151 de 2008 (por el cual se

establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.). En el cual se establecieron cinco (5) fases que concluían en el año 2012.

- Información en línea
- Interacción en línea
- Transacción en línea
- Transformación en línea
- Democracia en línea

Pero la importancia de citar este caso se centra en los mecanismos de implementación en el sector público, donde se la da verdadera importancia al tema de la seguridad de la información pública. Pero deja, su puesta en servicio en las manos de cada ente territorial, el cual debe proveer tanto el equipamiento como el recurso humano para su operación. La pregunta: ¿Cómo las harán los municipios donde su presupuesto para apropiación de nuevas tecnologías no existe o si existe es mínimo?

Por ello, el contraste es nada favorable para lo que se observa desde afuera, que el país tiene normas ha desarrollado políticas pero estas aún no se han implementado y aún más grave en muchos espacios de participación ciudadana se conocen.

6.3. CAPITULO III: panorama actual de la seguridad informática del país y tendencias futuras con la ciberseguridad.

¿Que se tiene como política pública?

En el año 2011, bajo el CONPES 3701, se establecieron las políticas públicas para la ciberseguridad y ciberdefensa, y solo hasta el año 2014, se procede a realizar la

primera revisión sobre los avances de dichas políticas. Lo primero que se encontró fue un desarrollo del 79%, y su ejecución corresponde a:

Tabla 2. Evaluación de la Política pública de seguridad.

Factor	Ejecución
Institucionalidad	"Creación de nuevas instancias tales como el Grupo de respuesta a emergencias cibernéticas de Colombia (colCERT) del Ministerio de Defensa Nacional, el Comando Conjunto Cibernético (CCOC) del Comando General de las Fuerzas Militares de Colombia, el Centro Cibernético Policial (CCP) de la Policía Nacional de Colombia, el Equipo de respuesta a incidentes de seguridad informática de la Policía Nacional (CSIRT PONAL), la Delegatura de protección de datos en la Superintendencia de Industria y Comercio, la Subdirección técnica de seguridad y privacidad de tecnologías de información del Ministerio de Tecnologías de la Información y las Comunicaciones, el Comité de ciberdefensa de las Fuerzas Militares, y las Unidades cibernéticas del Ejército Nacional, la Armada Nacional y la Fuerza Aérea Colombiana."
Capacitación	• colCERT • CCOC • CCP • Universidades e instituciones educativas
Legislación	• Ley 1581 de 2012
Cooperación y posicionamiento internacional	• Adhesión a la Convención de Europa sobre cibercriminalidad, también conocido como Convenio de Budapest • Comité Interamericano Contra el Terrorismo (CICTE) de la Organización de Estados Americanos (OEA), se ha logrado trabajar con varios Equipos de respuesta ante incidencias de seguridad (CSIRT) en la región.

	• Acuerdos con organizaciones internacionales como el Antiphishing Working Group • Ocho (8) CSIRT: FIRST (La principal organización mundial y líder reconocido en respuesta a incidentes digitales)

Fuente Propia

El estado reconoce: "… los resultados no pueden interpretarse como una capacidad suficiente, integral y efectiva de preparación y respuesta ante ataques cibernéticos. Esto, por la continua evolución, crecimiento y sofisticación de los ataques cibernéticos, que ponen de manifiesto la necesidad de adoptar nuevas medidas y controles que permitan proteger a los ciudadanos y al Estado."

Luego, aun cuando la política establecida, solamente se ha quedado en la creación de organismos que, para nada, se encuentran articulados pero que cada uno de ellos tienen un quehacer especifico. Es tal vez, una de las debilidades mayores frente a las amenazas de ataques cibernéticos. Que cada día han evolucionado y son muchas más letales.

Si se revisan los informes mundiales, Colombia permanece dentro de los 20 países de mundo más atacados. En la ilustración 3, es una muestra de esta información.
Definiciones de la ilustración:

- OAS (On-Access Scan) muestra el flujo de detección de malware durante el escaneo On- Access, por ejemplo, cuando los objetos son accesados durante las operaciones abrir, copiar, ejecutar o guardar operaciones.
- ODS (On Demand Scanner) muestra el flujo de detección de malware durante el análisis bajo pedido, cuando el usuario selecciona manualmente la opción "Buscar virus" en el menú de contexto.

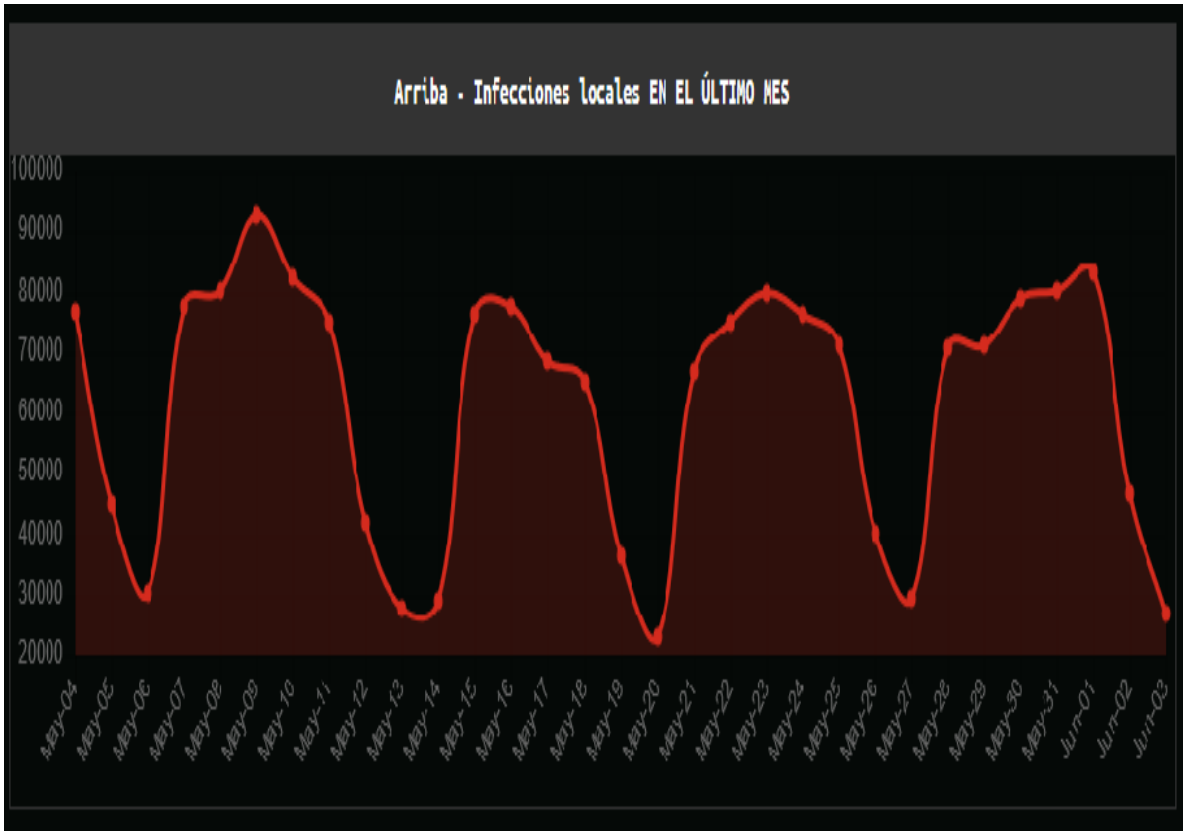
Ilustración 3. Colombia y los ataques informáticos

. Fuente: https://cybermap.kaspersky.com/es/

- MAV muestra el flujo de detección de malware durante el escaneo MAV cuando aparecen nuevos objetos en una aplicación de email (Outlook, The Bat, Thunderbird). MAV escanea los mensajes entrantes y llama a OAS cuando guarda los adjuntos a un disco.
- WAV (Web Anti-Virus) muestra el flujo de detección de malware durante el análisis Web Anti-Virus donde la página html de un sitio web se abre o un archivo es descargado.
- IDS (Sistema de Detección de Intrusos) muestra el flujo de detección de los ataques a las redes.
- VUL (Vulnerability Scan) muestra el flujo de la detección de vulnerabilidades.

- KAS (Kaspersky Anti-Spam) muestra el tráfico sospechoso y no deseado descubierto por las tecnologías de Filtrado de Reputación de Kaspersky Lab.
- BAD (Detección de Actividad Botnet) muestra estadísticas sobre direcciones IP de víctimas de ataques DDoS y servidores botnet C&C. Estas estadísticas fueron adquiridas con la ayuda del sistema de inteligencia DDoS.

Ilustración 4. Reporte de los ataques recibidos en Colombia durante el mes de mayo 2018.



Fuente: https://cybermap.kaspersky.com/es/stats#country=184&type=oas&period=m

Ilustración 5. Las infecciones en el mes de mayo/2018.

Arriba - Infecciones locales EN EL ÚLTIMO MES		
1	DangerousObject.Multi.Generic	12.71%
2	Trojan.Script.Generic	7.57%
3	Trojan.WinLNK.Agent.gen	6.43%
4	Trojan.WinLNK.Starter.gen	5.89%
5	Trojan.Script.Miner.gen	5.74%
6	HackTool.Win32.KMSAuto.m	4.97%
7	Trojan.WinLNK.Agent.sq	4.86%
8	Virus.Win32.Renamer.j	4.76%
9	Trojan.WinLNK.Agent.qk	4.18%
10	HackTool.Win32.KMSAuto.c	3.3%

Fuente: https://cybermap.kaspersky.com/es/stats#country=184&type=oas&period=m

Frente a esta situación desde el 2014 el Gobierno en un intento por mejorar la ciberseguridad y la ciberdefensa establece una Comisión de alto nivel para que construya y fortalezca las políticas públicas. Como resultado de ese trabajo, se obtiene el CONPES 3854 de 2016.

Se determinan cinco (5) dimensiones:

a. Gobernabilidad y coordinación efectiva;
b. Preparación y prevención;
c. Conocimiento de la situación actual;
d. Resiliencia, recuperación y respuesta;
e. Efectiva cooperación e intercambio de información (OEA, 2014).

Asimismo, se establecen cinco (5) recomendaciones enfocadas a la necesidad de:

a. Desarrollar una visión estratégica global para la ciberseguridad;
b. Adoptar un enfoque nacional de la gestión de riesgos;

c. Establecer un marco institucional claro;
d. Establecer un proceso sistemático para involucrar a todos los interesados en el desarrollo de la estrategia y su implementación; y
e. Adoptar una estrategia para la protección y defensa de las infraestructuras críticas cibernéticas nacionales, siendo conscientes de la necesidad de fortalecer las capacidades operativas, administrativas, humanas, científicas, tecnológicas y de infraestructura física de las instituciones (OEA, 2014).

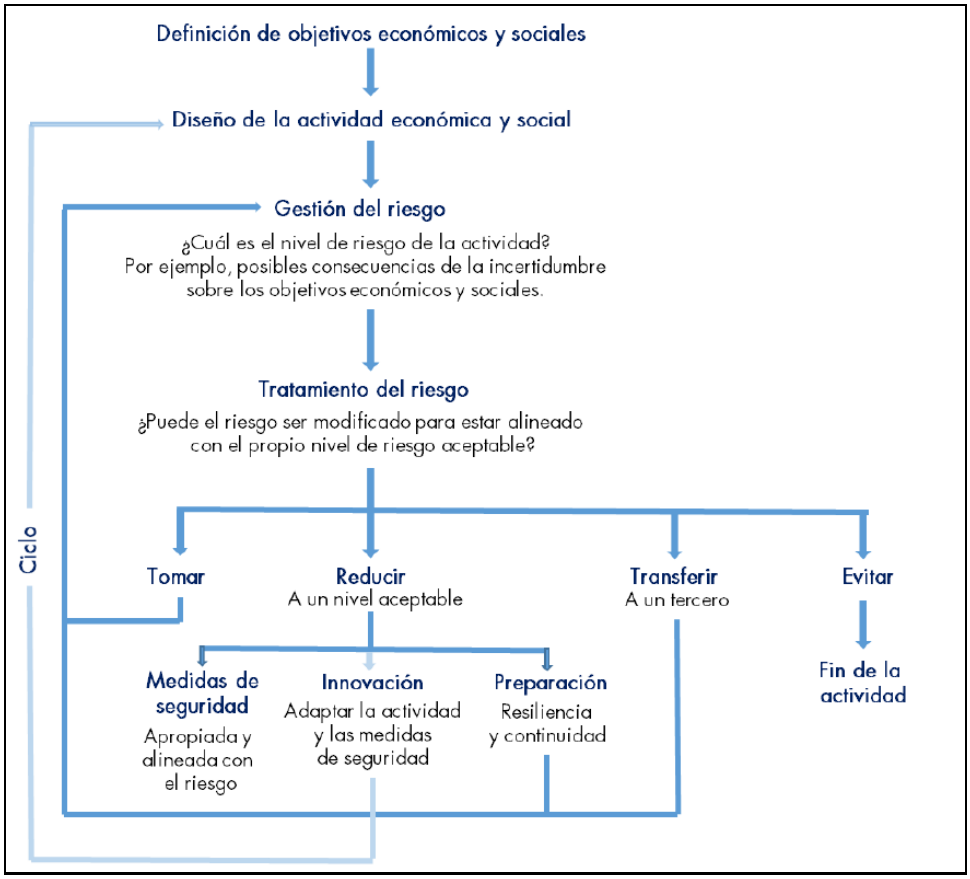
Como resumen de las políticas públicas, a partir de las recomendaciones de la OCDE: “la estrategia nacional debe ser consistente con el conjunto de principios formulados, debe crear las condiciones para que las múltiples partes interesadas puedan gestionar la seguridad digital de sus actividades económicas y sociales, debe fomentar la confianza en el entorno digital y, además, debe:

(i) estar apoyada desde el más alto nivel de gobierno;
(ii) afirmar claramente que su objetivo es aprovechar el entorno digital abierto para la prosperidad económica y social;
(iii) estar dirigida a todas las partes interesadas; y
(iv) ser el resultado de un enfoque intragubernamental, coordinado, abierto y transparente, donde participen las múltiples partes interesadas.”

La ilustración 6 muestra una representación genérica de la gestión sistemática y cíclica de riesgos de seguridad digital, reflejando los principios operativos de la recomendación de la OCDE. Esta inicia con la definición de un objetivo o el diseño de una actividad, luego, en la etapa conocida como gestión del riesgo, se evalúa cuál es el nivel de riesgo de dicha actividad determinando todos los resultados posibles de asumirlo sobre los objetivos sociales y económicos. Posteriormente, en la etapa de tratamiento del riesgo, se determina cómo debería ser modificado el mismo, con el fin de aumentar la probabilidad de éxito de la actividad y preservar

los objetivos definidos, decidiendo si el riesgo debe ser tomado, reducido, transferido o evitado. Si se decide reducirlo, se pueden seleccionar y aplicar medidas de seguridad, se puede considerar la innovación, o las medidas de preparación para su tratamiento.

Ilustración 6. Modelo de gestión sistemática y cíclica de riesgo de seguridad digital.



Fuente: OCDE (2015a).

Luego el documento CONPES define: “Así las cosas, la política nacional de seguridad digital:

(i) adoptará la gestión sistemática y cíclica del riesgo;

(ii) será liderada desde el alto nivel del gobierno;

(iii) asegurará la defensa y seguridad nacional;

(iv) estimulará la prosperidad económica y social;

(v) adoptará un enfoque multidimensional, es decir, la seguridad digital será abordada tanto desde la dimensión técnica o jurídica, como desde la dimensión económica y social;

(vi) tendrá en cuenta a las múltiples partes interesadas;

(vii) promoverá la responsabilidad compartida;

(viii) salvaguardará los derechos humanos;

(ix) protegerá los valores nacionales; y

(x) concientizará y educará."

Bajo estas perspectivas, el gobierno establece los principios fundamentales de la política nacional de seguridad digital:

Tabla 3. Principios fundamentales de la política nacional de seguridad digital

Principio	Definición
PF1	Salvaguardar los derechos humanos y los valores fundamentales de los ciudadanos en Colombia, incluyendo la libertad de expresión, el libre flujo de información, la confidencialidad de la información y las comunicaciones, la protección de la intimidad y los datos personales y la privacidad, así como los principios fundamentales consagrados en la Constitución Política de Colombia. En caso de limitación a estos derechos, debe ser bajo medidas excepcionales y estar conforme con la Constitución Política y los estándares internacionales aplicables. Estas medidas, deben ser proporcionales, necesarias y estar enmarcadas en la legalidad.
PF2	Adoptar un enfoque incluyente y colaborativo que involucre activamente a las múltiples partes interesadas, y que permita establecer condiciones para el desarrollo eficiente de alianzas, con el fin de promover la seguridad digital del país y sus habitantes, y aumentar la capacidad de resiliencia nacional frente a eventos no deseados en el entorno digital.
PF3	Asegurar una responsabilidad compartida entre las múltiples partes interesadas, promoviendo la máxima colaboración y cooperación. Lo anterior, teniendo en cuenta el rol y el grado de responsabilidad de cada parte para gestionar los riesgos de seguridad digital y para proteger el entorno digital.

PF4	Adoptar un enfoque basado en la gestión de riesgos, que permita a los individuos el libre, seguro y confiable desarrollo de sus actividades en el entorno digital. Lo anterior, fomentará la prosperidad económica y social, buscando la generación de riqueza, innovación, productividad, competitividad, y empleo en todos los sectores de la economía.

Fuente Elaboración Propia

Bajo esos principios rectores se definen las dimensiones estratégicas:

Tabla 4. Dimensiones estratégicas.

Dimensión	Descripción
DE 1	Gobernanza de la seguridad digital: articulación y armonización de las múltiples partes interesadas, bajo un marco institucional adecuado, con el fin de gestionar la seguridad digital, bajo el liderazgo del Gobierno nacional.
DE 2	Marco legal y regulatorio de la seguridad digital: marco legal y regulatorio que soporta todos los aspectos necesarios para adelantar la política.
DE 3	Gestión sistemática y cíclica del riesgo de seguridad digital: conjunto de iniciativas, procedimientos o metodologías coordinadas con el fin de abordar, de manera cíclica y holística, los riesgos de seguridad digital en el país.
DE 4	Cultura ciudadana para la seguridad digital: sensibilización de las múltiples partes interesadas, para crear y fomentar una cultura ciudadana responsable en la seguridad digital.
DE 5	Capacidades para la gestión del riesgo de seguridad digital: fortalecimiento y construcción de capacidades humanas, técnicas, tecnológicas, operacionales y administrativas en las múltiples partes interesadas, para adelantar la gestión de riesgos de la seguridad digital.

Fuente Elaboración Propia

De esto que se deduce, el estado propicia una política amplia, basada en un enfoque multidimensional donde caben todos los actores que debe responder y velar por la seguridad informática y de la información.

6.4. CAPITULO IV: Tendencias futuras con la ciberseguridad

Pero, ¿Que nos queda? Si se observa existe un factor donde se incorpora a cada uno de los ciudadanos, desde el modelo de la OCDE, concientizará y educará; desde el principio PF 3, de la responsabilidad compartida; y desde la dimensión estratégica DE 4, Cultura ciudadana para la seguridad digital.
Si se revisan y comparan las propuestas de la OCDE con las propuestas de la UNESCO, frente al estudiante del siglo XXI, se tiene una analogía en una estrategia válida y de una aplicación inmediata: el AUTO-CUIDADO. Para la UNESCO, se refiere al cuidado de la salud física y se podrá incluir la salud mental. Lo que es, si el ciudadano de a pie, comprende la importancia de la seguridad para su vida.

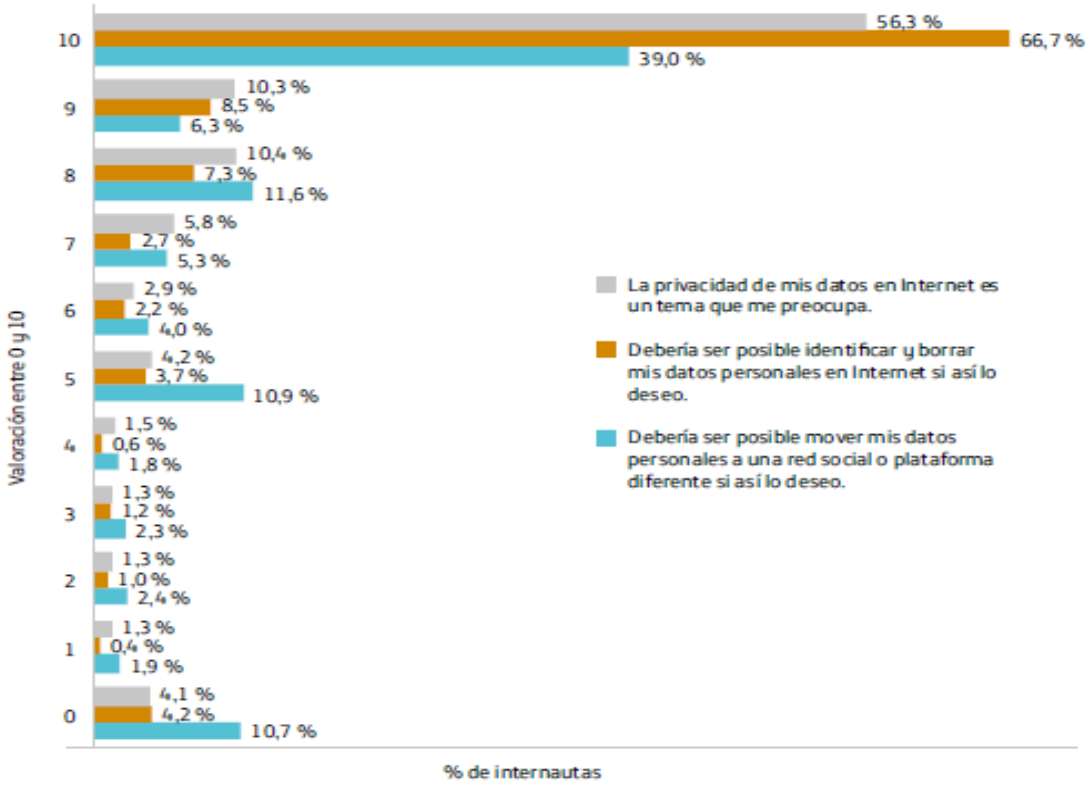
Algunos autores sobre temas de seguridad informática, advierten que el punto más débil de la cadena de seguridad es el ser humano, su actitud frente a los compromisos de la seguridad digital. Fundación Telefónica (2016, pg. 10) dice: “Este proceso de digitalización de los servicios y de la economía en general implica importantes retos que conciernen a diferentes elementos del ecosistema digital. De entre los usuarios, las empresas suelen tener una mayor capacidad para afrontar estos retos, ya que disponen de más recursos y suelen contar con especialistas en tecnologías de la información, por ese motivo el internauta individual se puede considerar la parte más débil de este ecosistema. En esta sección analizamos la percepción de los usuarios ante la seguridad, las amenazas que se presentan hoy y las medidas que los usuarios toman ante esta situación”

En los estudios realizados por la Fundación Telefónica han obtenido:

1. Factor: Percepción de los usuarios ante la seguridad y privacidad en Internet (valoración entre 0 y 10)

En la ilustración 7, se puede observar que con la máxima valoración (10) los usuarios han calificado las características de este factor, en un 56,3% Consideran que la privacidad de los datos les preocupa, un 66,7% que debería ser posible identificar y borrar los datos personales se así lo desea y con un 39%, consideran que debe ser posible mover los datos personales a una red o plataforma diferente si lo desea.

Ilustración 7. Percepción de los usuarios ante la seguridad y privacidad en Internet.



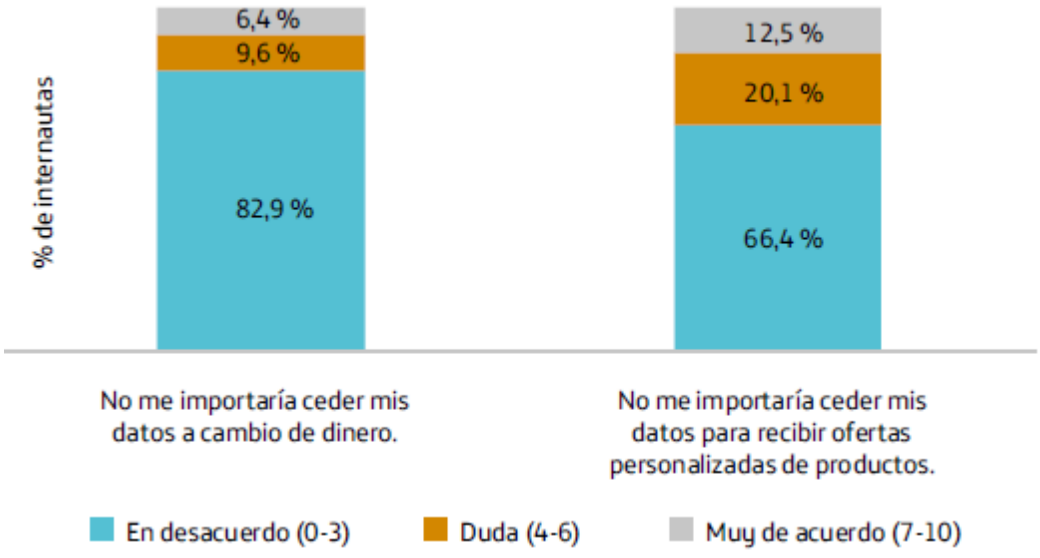
Fuente Fundación Telefónica

Visto en conjunto para este primer factor, el usuario tiene conciencia de la protección y del uso de sus de sus datos. Pero, también se percibe que no es un indicador fiable al observar que la valoración está entre los 7 y los 10 puntos.

2. Factor: Actitudes ante la cesión de datos personales para obtener beneficios**.**

Los resultados obtenidos por la Fundación Telefónica, son los de la Ilustración 8 y se observa una actitud mucha más segura frente a este factor y sus dos (2) características. Pero con un síntoma de alto riesgo, a los internautas si estarán dispuestos a ceder los datos para recibir ofertas personalizadas de productos (66,4%). Aquí, entonces aparecen los compromisos éticos de las empresas que hacen uso de estas estrategias de mercadeo y la ingenuidad de los clientes frente a empresas nada confiables.

Ilustración 8. Actitudes ante la cesión de datos personales para obtener beneficios.



Fuente Fundación Telefónica.

3. Factor: Ciberamenazas a la privacidad de los usuarios

En el documento de la Fundación Telefónica (2016), expresa sobre este factor: “Los usuarios presentan una actitud de preocupación e interés ante estos temas, aunque, según se mostrará más adelante, en muchas ocasiones no son capaces de identificar cuáles son los peligros y por tanto no saben cómo enfrentarse a ellos. Una primera medida en este sentido será el conocer cómo el *malware* llega hasta nuestros sistemas, que deberá condicionar nuestro comportamiento; por ejemplo, no seguir cadenas de correos, utilizar *software* de fuentes seguras, tener cuidado al introducir USB de terceras personas… y es que los medios de distribución de *software* dañino son cada vez más variados.

A esta situación ha de añadirse que la naturaleza y los objetivos de los ataques cibernéticos han ido cambiando con el tiempo. Por ejemplo, la mayoría de los usuarios piensa que los atacantes van a ir detrás de información suya, ya sea personal o claves. No obstante, en muchas ocasiones, el objetivo de los atacantes es acceder a los recursos del usuario, como aprovechar el poder de procesamiento para realizar tareas que requieran gran poder de computación, como realizar *bitcoin mining*. Otro ejemplo sería el de acceder a su ancho de banda para que su sistema actúe como un zombi dentro de una *botnet* y poder realizar ataques masivos.

Es posible que el usuario considere que no tiene ninguna información relevante que pueda ser utilizada por delincuentes. Eso suele ser una percepción falsa, ya que los atacantes pueden querer acceder a las libretas de contactos para realizar spam masivo personalizado y atacar a terceras personas, o bloquear el ordenador y pedir un rescate por recuperar la información, pues, aunque la información no sea de valor para terceras personas, sí lo será para el propio usuario.

Los robos más importantes de información pueden afectar a tres tipos de aspectos:

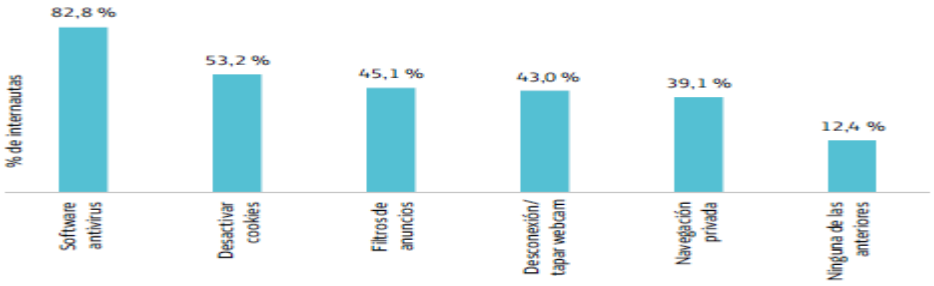
- *Económico*: si te roban las contraseñas o tienen acceso a sistemas online como bancos, Paypal, bitcoins…
- *Lúdico*: se refiere a la pérdida de fotografías, acceso a información sensible como repositorios en la nube…
- *De «imagen»:* si roban cuentas de las redes sociales, pueden llegar a suplantar la identidad y dañarla.

Es necesario que los usuarios sean conscientes de las nuevas normas de juego que imponen Internet y las nuevas tecnologías y conozcan tanto los mecanismos más importantes que utilizan los atacantes como cuáles de nuestras identidades pueden ser interesantes para ellos."

4. Factor: Medidas relacionadas con privacidad y seguridad tomadas por los usuarios

Los nuevos cambios tecnológicos, con la penetración masiva de Internet ha obligado a muchos usuarios a tomar medidas de protección frente a las amenazas de ataques. Pero, no es lo suficiente, porque no se han apropiado de esta situación debería suponer una transformación completa de las medidas y actitudes que los usuarios tomaran en referencia a la privacidad y seguridad en su mundo digital. Hoy, todavía, el usuario depende mayormente del software antivirus. La Ilustración 9, nos muestra los resultados de la encuesta de Fundación Telefónica en el año 2015.

Ilustración 9. Medidas para proteger la privacidad tomadas por los internautas.



Fuente Fundación Telefónica.

La discusión se debe centrar en por qué el usuario, hoy no le está dando la importancia que debe tener la seguridad de la información. Pero, no debemos centrarnos en el problema sino en la búsqueda de una solución coherente y aplicable.

El estado, ha establecido unas estrategias, donde unos de los elementos más importantes están centrados en la capacitación y en la formación de personal idóneo. Esto es, la responsabilidad compartida y la cultura ciudadana. Ahora se deberá definir el cómo se hace.

En los modelos educativos, se imparte abiertamente el uso de las herramientas digitales y el conocimiento del computador. Pero no se está, profundizando en los cuidados que debe tener un niño, joven o adulto cuando hace uso del internet. Luego, desde una visión de Gobierno, este deberá propender bajo los programas académico a estimular la seguridad de la información y de los dispositivos informáticos para crear una cultura permanente que garantice que las políticas que se adopten logren los objetivos de la seguridad de la información y de la seguridad informática.

“El usuario de momento vive feliz. Solo se le remueve la conciencia cuando sale el caso de Snowden, cuando hay un robo de 4 millones de contraseñas. Pero no pasa absolutamente nada, seguimos usando el mismo servicio, la misma contraseña. Yo lo sigo haciendo. Por tanto, fijaos en el nivel de inconsistencia.” Palabras del *Presidente de la Asociación de Usuarios de Internet, española,* MIGUEL PÉREZ SUBÍAS.

Que se podrá decir frente a esta afirmación, cuál es hoy nuestro nivel de inconsistencia en los temas relacionados con la seguridad de la información y de los recursos informáticos.

Con el aumento de aplicaciones para los teléfonos móviles, donde muchas de ellas, piden que se permita el uso de nuestros datos y de forma inconsciente damos esos permisos, que más tarden traerán graves problemas de nuestra información.
Debemos plantearnos las mismas preguntas que formuló la Fundación Telefónica a muchos expertos:

- ¿Qué percepción tienen los usuarios de la seguridad en los servicios digitales?
- ¿Qué están haciendo los usuarios para protegerse?

La respuesta estará en los criterios y la información que cada usuario tenga sobre la seguridad de la información y la seguridad informática.

7. RESULTADOS E IMPACTOS ESPERADOS

Solamente en el presente siglo, el Estado ha comprendido la importancia de la seguridad de la información y es por ello, que se han expedido dos (2) CONPES y se ha promulgado una Ley, pero esta, más orientada a los derechos de autor. Los vacíos jurídicos que hoy se observan van desde el uso de algunas aplicaciones hasta plataformas de servicios telemáticos; las cuales funcionan libremente con una alta indisposición de la ciudadanía y del sector empresarial del País, ejemplo: el servicio UBER.

La política de Gobierno Digital tiene como ámbito de aplicación las entidades que conforman la Administración Pública en los términos del artículo 39 de la Ley 489 de 1998 y los particulares que cumplen funciones administrativas. La implementación de la Política en las Ramas Legislativa y Judicial, en los órganos de control, en los autónomos e independientes y demás organismos del Estado, se realizará bajo un esquema de coordinación y colaboración armónica en aplicación de los principios señalados en el artículo 209 de la Constitución Política.

Así mismo, con el objetivo de identificar claramente los roles para la implementación de la Política de Gobierno Digital, se definió un esquema institucional que vincula desde la alta dirección hasta las áreas específicas de la entidad, en el desarrollo de la política y el logro de sus propósitos.

Si se revisa el nivel de penetración en la aplicación de la política de Gobierno en línea, para este año, se había previsto que todas las entidades territoriales deberían haberlo implementado, en especial el componente de la seguridad de la información. En Ministerio de las TIC reconoce que solamente en un 66% se ha logrado dar inicio al proceso.

Se puede concluir que no existe un seguimiento por las organizaciones creadas en el tema concreto de la seguridad de la información y la protección a los ciberataques. Aun cuando existen organizaciones internacionales que apoyan a la seguridad informática en el país, la cultura ciudadana y las políticas están muy por debajo de las expectativas internacionales.

El mundo se ha ido organizando en frentes unificados para la protección del cibercrímen. Pero es fundamental, la consolidación de las políticas públicas y la formación y educación de todos y cada uno de los usuarios y/o ciudadanos.

8. CONCLUSIONES

- En materia de normatividad del País frente a la Ciberseguridad, Colombia está reconocida por los miembros de la OEA como uno de los países que más avanzado en la implementación. No basta con las políticas públicas establecidas, sino como se están implementando y como permea las acciones del mismo estado en sus diferentes niveles o entes territoriales. Asimismo, esta política deberá fomentar las relaciones internacionales a partir que el Ciberespacio no requiere de fronteras físicas.

- Que la normatividad no incorpora de forma concreta y permanente a las empresas privadas que hoy tienen un alto porcentaje en el manejo de las infraestructuras criticas del País. Es probable que ellas, las empresas privadas, tengan incorporadas a sus operaciones políticas de Ciberseguridad, pero esto no es una garantía, sino están interrelacionadas con el Estado y con el Gobierno.

- La normatividad debe ser compartida en todos y cada uno de los diferentes escenarios de participación ciudadana para que sea apropiada por el común de la gente. Como un elemento de la Cultura ciudadana. Está la importancia de establecer programas a todo nivel, para la capacitación en estos temas de seguridad de la información. Esto es, se puede observar que una Estrategia Nacional de Ciberseguridad debe ser un instrumento que guíe a los responsables de la dirección y gestión de la Ciberseguridad Nacional y que involucre a todas las organizaciones públicas o privadas y a la sociedad para trabajar en coordinación, además debe servir como instrumento que contribuye a la defensa y debe definir una visión estratégica basada en los

pilares de responsabilidad y Política. Que dependen fundamentalmente del Gobierno.

- El Gobierno central debe de disponer todos los recursos necesarios para que los entes territoriales con mínima capacidad financiera puedan apropiar, implementar y operar los sistemas informáticos dentro de los más altos grados de seguridad, cuando se reconoce que la información pública es un bien y es de todos.

- En el estado actual de la seguridad del país, se observa que las entidades que manejan grandes volúmenes de información, en espacial los sectores financieros, han realizado grandes inversiones. Pero no por ello, siguen siendo objeto de ataques de todo tipo. Es claro ver en el mapa de Ciberamenazas en tiempo real de la firma Kaspersky (https://cybermap.kaspersky.com/es), muestra a Colombia como uno de los países con mayor número de amenazas y se ubica entre los 20 primeros países del mundo. Luego, es urgente y necesario un verdadero plan de acción que involucre desde los ciudadanos comunes hasta las grandes empresas en la construcción colectiva de una cultura ciudadana para la Ciberseguridad.

- Como tendencia de Ciberseguridad se debe tener en cuenta que la incertidumbre es un ingrediente que aporta variables imprevisibles, debido a la dificultad de conocer de antemano el total de las amenazas y riesgos a los que se enfrenta la sociedad en cada situación, dificultando con ello la selección de medidas para combatirlas, además de una actitud reactiva frente a estos hechos. Luego se debe intentar priorizar sobre los riesgos y las amenazas existentes para hacerles frente de forma eficaz, involucrando a todos y cada uno de los actores fundamentales, junto con las reales y crecientes vulnerabilidades derivadas, principalmente de las interdependencias propias de un mundo globalizado, que contribuyen a introducir un alto nivel de incertidumbre en la seguridad y la capacidad de las infraestructuras para

soportar los efectos de los riesgos. Como elemento final: “En este entorno de globalización, la respuesta oportuna está condicionada por el concepto de resiliencia, que muestra su verdadero valor al complementar y facilitar las propuestas y respuestas más eficaces y adecuadas. Para disminuir nuestras vulnerabilidades, hay que moverse y no sucumbir al miedo ni a la autocomplacencia aumentando esa “capacidad de adaptación de un ser vivo frente a un agente perturbador o un estado o situación adversos” que la definen.”[4]

[4] Blog sobre convergencia y tecnología de Tendencias21. https://www.tendencias21.net/seguridad/

9. RECOMENDACIONES

- Hoy se deben responder los siguientes interrogantes frente a la Ciberseguridad: ¿Cómo dominar el control de la gestión de riesgos y de la continuidad del negocio o funcionamiento frente a un Ciberataque? y ¿Cómo mejorar la adaptabilidad y lograr un equilibrio aceptable y sostenible entre los riesgos, la complejidad y los costes si los requisitos de seguridad y conformidad son cada vez mayores?, teniendo en cuenta que se debe tener conformidad (Excesos de restricciones/ o de políticas de control en la red que la ralentizan): con las amenazas cambiantes; las normativas cambiantes; las tecnologías cambiantes; la economía cambiante; los requisitos de las infraestructuras cambiantes.

- En definitiva, las infraestructuras deberán adaptarse cada vez con más rapidez a las condiciones cambiantes de su entorno. Un caso de especial cuidado es la industria, ella es muy vulnerable. Generalmente no se está preparado para enfrentar las amenazas cibernéticas, técnicamente, organizativamente, u operativamente. Las amenazas se están expandiendo e intensificando.

- Todas las fuerzas impulsoras del cambio descritas anteriormente hacen que la seguridad y la conformidad sean unos objetivos, unos retos difíciles de lograr su adecuada planificación. Estas serán, especialmente, responsabilidades de los CIO’s para equilibrar los riesgos, la complejidad y los costes.

- En el ámbito académico estos nuevos desafíos implican fomentar la capacitación para la complejidad y el cambio permanente. Esto impone partir reconociendo que sólo a través de la intersección de diferentes disciplinas de

la seguridad y la defensa seremos capaces de posibilitar la visión holística, es decir, de la participación público-privada. Responder a una reinvención y evolución de los riesgos y amenazas requiere, obligatoriamente, de un capital humano formado para la complejidad. Esto lleva a promover un modelo de capacitación especializada que ponga al sujeto proactivamente en el centro de su formación y fortalezca las competencias genéricas y profesionales en las que se enmarcan el saber hacer y emprender de un especialista en esta área.

- Existen muchos escenarios para la continuación de este trabajo, entre ellos, la industria o el sector empresarial. No se está preparado para resistir los ciberataques. Las regulaciones del gobierno reflejan un requisito mínimo para las empresas, en el que las obliguen a proteger la información. La mayoría de las empresas no adoptan un marco regulatorio estable para proteger sus infraestructuras críticas (ICIs) y el nivel de conciencia es bajo, lo que las hace aún más vulnerables a los ciberataques.

- Otro escenario posible está en las evaluaciones inadecuadas de los riesgos. Hoy no llevan a cabo unas evaluaciones de riesgos significativas y a menudo las evaluaciones de riesgos que se llevan a cabo, son realizadas por personal que carece de suficiente perspectiva, conocimiento y experiencia. Las evaluaciones de riesgos inadecuadas pueden ser particularmente peligrosas porque infunden una falsa sensación de seguridad. Una falsa sensación de seguridad puede conducir a consecuencias devastadoras.

BIBLIOGRAFÍA

ACOSTA PASTOR, Oscar; *et al*. (2009). Seguridad nacional y ciberdefensa (1a.ed.). Madrid: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones.

AVILÉS, Ángel Pablo, LARRAÑAGA Kepa Paul, [online]. Ed. 2015 Aranzadi Atención mamás y papás. Pamplona España. ISBN: 9788490989784.

---------- [online].1 Ed. mayo 2013 X1Red+Segura – Informando y Educando – v.1.0. Madrid España. TO-326-2013.

BRUCE, Dang, (2014**)** Ingeniería Inversa Práctica: x86, x64, ARM, Windows Kernel, Herramientas de Inversión, y Ofuscación

BOGOTA. DEPARTAMENTO DE PLANEACIÓN NACIONAL (2016) POLÍTICA NACIONAL DE SEGURIDAD DIGITAL. CONPES 3854.

DOWD, Mark; MCDONAL Jhon; SCHUH, Justin (2006) El Arte de la Valoración de Seguridad de Softwares: Identificando y Previniendo Vulnerabilidades de Software. https://www.amazon.com/The-Software-Security-Assessment-Vulnerabilities/dp/0321444426/

FUNDACIÓN TELEFÓNICA (2016) Ciberseguridad, la protección de la información en un mundo digital. Editorial ARIEL. Recuperada de: https://www.fundaciontelefonica.com/arte_cultura/publicaciones-listado/pagina-item-publicaciones/itempubli/531/

GOBIERNO EN LÍNEA (2018) Estrategia de gobierno en línea. Recuperado de: http://estrategia.gobiernoenlinea.gov.co/623/w3-channel.html

LEIVA, Eduardo Alfredo (2015) Estrategias Nacionales de Ciberseguridad: Estudio

Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. Revista Latinoamericana de Ingeniería de Software, 3(4): 161-176, ISSN 2314-2642. Recuperado de: http://revistas.unla.edu.ar/software/article/view/775/826

MINTIC (2015) Estudio exploratorio prospectiva de la industria TI en Colombia. Recuperado de https://colombiatic.mintic.gov.co/679/articles-73973_recurso_1.pdf

MONTERO GOMEZ, Andrés. (2006) Inteligencia Prospectiva de Seguridad. Documento de trabajo. Recuperado de: https://core.ac.uk/download/pdf/42965794.pdf

NASSIM, Nicholas Taleb (2008) El Cisne Negro. El impacto de lo altamente improbable. Barcelona: Paidós. Primera edición**.**

OCDE (2016) Evaluar el impacto del gobierno digital en Colombia. Recuperado de: https://www.oecd.org/countries/colombia/evaluar-el-impacto-del-gobierno-digital-en-colombia-9789264284272-es.htm

OCDE (2002) Guías de la OCDE para la seguridad de los sistemas de información y redes. Hacia una cultura de seguridad.

PETER Szor (2005) El Arte de la Investigación y Defensa en los Virus de Computadora. https://www.amazon.com/The-Computer-Virus-Research-Defense/dp/0321304543/

RAUSCHER, Karl; YASHENKO, Valery. (2011) The Russia--U.S. Bilateral on Cybersecurity – Critical Terminology Foundations. Recuperado de: https://www.files.ethz.ch/isn/130080/Russia-U%20S%20%20bilateral%20on%20terminology%20v76%20(2)-1.pdf

SALAS, Antonio. Editorial: S.L.U. ESPASA LIBROS (2015) Los hombres que le susurran a las maquinas. Hackers, espías e intrusos en tu ordenador. ISBN:

9788467049336.

SHOSTACK Adam; (2014) Modelando Amenazas: Diseñando para Seguridad**.** https://www.amazon.com/Threat-Modeling-Designing-Adam-Shostack/dp/111880998

VILLALÓN HUERTA, Antonio (2004) Códigos de buenas prácticas de seguridad. UNE/ISO/IEC 17799. Recuperado de: http://www.shutdown.es/ISO17799.pdf

RESUMEN ANALITICO EDUCATIVO

RAE

Título del texto	Panorama actual de la seguridad informática o de la ciberseguridad, a nivel del país y las tendencias actuales y futura a nivel global
Nombres y Apellidos del Autor	Hernando Arbey Robles Puentes
Año de la publicación	**2018**

Resumen del texto:

Apenas hace unos pocos años, se ha iniciado la cultura de la seguridad informática, las organizaciones antes del año 2000 invertían mucho más en café y bebidas que en seguridad. Las tecnologías emergentes en el presente siglo, han superado cualquier pronóstico de penetración en todos los ámbitos sociales, culturales, económicos y políticos. Y con ello, han proliferado cualquier cantidad de ataques a la información de Gobiernos, de empresas y de personas. Lo que ha influenciado que muchos gobiernos, agencias multilaterales y empresas hayan tomado partido por la seguridad informática.

Frente a este hecho, ampliamente reconocido, los estados y las políticas gubernamentales han estado un paso atrás. En Colombia, solamente en el 2016, se produce la modificación al CONPES 3701/11, documento integral sobre seguridad digital y es a través del CONPES 3854, y en uno de sus apartes expresa:

> "El enfoque de la política de ciberseguridad y ciberdefensa, hasta el momento, se ha concentrado en contrarrestar el incremento de las amenazas cibernéticas bajo los objetivos de (i) defensa del país; y (ii) lucha contra el cibercrímen. Si bien esta política ha posicionado a Colombia como una de los líderes en la materia a nivel regional, ha dejado de lado la gestión del riesgo en el entorno digital.
>
> Enfoque esencial en un contexto en el que el incremento en el uso de las TIC para realizar actividades económica s y sociales, ha traído consigo nuevas y más sofisticadas formas de afectar el desarrollo normal de estas en el entorno digital. Hecho que demanda una mayor planificación, prevención, y atención por parte de los países."

La propuesta gubernamental es que para el año 2020 este la política implementada. Lo cual muestra, un periodo de emergencia, cuando no todos los actores están comprometidos con el establecimiento de lineamientos sobre la ciberseguridad. A partir de este escenario, es importante realizar un estudio que

determine un panorama mucho más profundo en la seguridad informática del país y comparado con lo que se ha desarrollado en otros países.	
Palabras Claves	Seguridad Informática, seguridad de la información, infraestructura crítica, Amenaza informática, Ciberespacio, Ciberdefensa, Ciberseguridad
Problema que aborda el texto: El terrorismo y la delincuencia organizada global no sólo han retado las tradicionales concepciones de seguridad interior y exterior, sino que están poniendo de manifiesto que la seguridad reactiva o que la seguridad desgajada de la inteligencia son respuestas obsoletas de los Estados ante las amenazas. El desarrollo de doctrina, métodos y órganos para la inteligencia prospectiva de seguridad se presenta como una opción estructural para proporcionar a las instituciones de seguridad capacidades de respuesta inteligentes, preventivas y proactivas ante las nuevas amenazas.	
Objetivos del texto: Describir el panorama actual de la seguridad informática o de la ciberseguridad, a nivel del país y las tendencias actuales y futura a nivel global.	
Hipótesis planteada por el autor: ¿Cuál es el panorama actual de la seguridad informática o de la ciberseguridad, a nivel del país y las tendencias actuales y futuras a nivel global?	
Tesis principal del autor: Es muy importante, trabajar e indagar como está el país, como está la construcción de una cultura de protección de la información, cuando la exponemos en programas de gobierno en línea, datos abiertos, e-gobierno, etc.	
Argumentos expuestos por el autor: La falta de una política pública clara y concreta sobre la seguridad de la información en todo su contexto. La normatividad existente es una normatividad reactiva a los eventos de amenazas cibernéticas en el País.	
Conclusiones del texto: • En materia de normatividad del País frente a la Ciberseguridad, Colombia está reconocida por los miembros de la OEA como uno de los países que más avanzado en la implementación. No basta con las políticas públicas establecidas, sino como se están implementando y como permea las acciones del mismo estado en sus diferentes niveles o entes territoriales. Asimismo, esta política deberá fomentar las relaciones internacionales a partir que el Ciberespacio no requiere de fronteras físicas. • Que la normatividad no incorpora de forma concreta y permanente a las empresas privadas que hoy tienen un alto porcentaje en el manejo de las infraestructuras criticas del País. Es probable que ellas, las empresas privadas, tengan incorporadas a sus operaciones políticas de Ciberseguridad, pero esto no es una garantía, sino están interrelacionadas con el Estado y con el Gobierno.	

- La normatividad debe ser compartida en todos y cada uno de los diferentes escenarios de participación ciudadana para que sea apropiada por el común de la gente. Como un elemento de la Cultura ciudadana. Está la importancia de establecer programas a todo nivel, para la capacitación en estos temas de seguridad de la información. Esto es, se puede observar que una Estrategia Nacional de Ciberseguridad debe ser un instrumento que guíe a los responsables de la dirección y gestión de la Ciberseguridad Nacional y que involucre a todas las organizaciones públicas o privadas y a la sociedad para trabajar en coordinación, además debe servir como instrumento que contribuye a la defensa y debe definir una visión estratégica basada en los pilares de responsabilidad y Política. Que dependen fundamentalmente del Gobierno.

- El Gobierno central debe de disponer todos los recursos necesarios para que los entes territoriales con mínima capacidad financiera puedan apropiar, implementar y operar los sistemas informáticos dentro de los más altos grados de seguridad, cuando se reconoce que la información pública es un bien y es de todos.

Bibliografía citada por el autor:

ACOSTA PASTOR, Oscar; et al. (2009). Seguridad nacional y ciberdefensa (1a.ed.). Madrid: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones.

AVILÉS, Ángel Pablo, LARRAÑAGA Kepa Paul, [online]. Ed. 2015 Aranzadi Atención mamás y papás. Pamplona España. ISBN: 9788490989784.

---------- [online].1 Ed. mayo 2013 X1Red+Segura – Informando y Educando – v.1.0. Madrid España. TO-326-2013.

BRUCE, Dang, (2014) Ingeniería Inversa Práctica: x86, x64, ARM, Windows Kernel, Herramientas de Inversión, y Ofuscación

BOGOTA. DEPARTAMENTO DE PLANEACIÓN NACIONAL (2016) POLÍTICA NACIONAL DE SEGURIDAD DIGITAL. CONPES 3854.

DOWD, Mark; MCDONAL Jhon; SCHUH, Justin (2006) El Arte de la Valoración de Seguridad de Softwares: Identificando y Previniendo Vulnerabilidades de Software. https://www.amazon.com/The-Software-Security-Assessment-Vulnerabilities/dp/0321444426/

FUNDACIÓN TELEFÓNICA (2016) Ciberseguridad, la protección de la información en un mundo digital. Editorial ARIEL. Recuperada de: https://www.fundaciontelefonica.com/arte_cultura/publicaciones-listado/pagina-

item-publicaciones/itempubli/531/

GOBIERNO EN LÍNEA (2018) Estrategia de gobierno en línea. Recuperado de: http://estrategia.gobiernoenlinea.gov.co/623/w3-channel.html

LEIVA, Eduardo Alfredo (2015) Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. Revista Latinoamericana de Ingeniería de Software, 3(4): 161-176, ISSN 2314-2642. Recuperado de: http://revistas.unla.edu.ar/software/article/view/775/826

MINTIC (2015) Estudio exploratorio prospectiva de la industria TI en Colombia. Recuperado de https://colombiatic.mintic.gov.co/679/articles-73973_recurso_1.pdf

MONTERO GOMEZ, Andrés. (2006) Inteligencia Prospectiva de Seguridad. Documento de trabajo. Recuperado de: https://core.ac.uk/download/pdf/42965794.pdf

NASSIM, Nicholas Taleb (2008) El Cisne Negro. El impacto de lo altamente improbable. Barcelona: Paidós. Primera edición.

OCDE (2016) Evaluar el impacto del gobierno digital en Colombia. Recuperado de: https://www.oecd.org/countries/colombia/evaluar-el-impacto-del-gobierno-digital-en-colombia-9789264284272-es.htm

OCDE (2002) Guías de la OCDE para la seguridad de los sistemas de información y redes. Hacia una cultura de seguridad.

PETER Szor (2005) El Arte de la Investigación y Defensa en los Virus de Computadora. https://www.amazon.com/The-Computer-Virus-Research-Defense/dp/0321304543/

RAUSCHER, Karl; YASHENKO, Valery. (2011) The Russia-¬-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations. Recuperado de: https://www.files.ethz.ch/isn/130080/Russia-U%20S%20%20bilateral%20on%20terminology%20v76%20(2)-1.pdf

SALAS, Antonio. Editorial: S.L.U. ESPASA LIBROS (2015) Los hombres que le susurran a las maquinas. Hackers, espías e intrusos en tu ordenador. ISBN: 9788467049336.

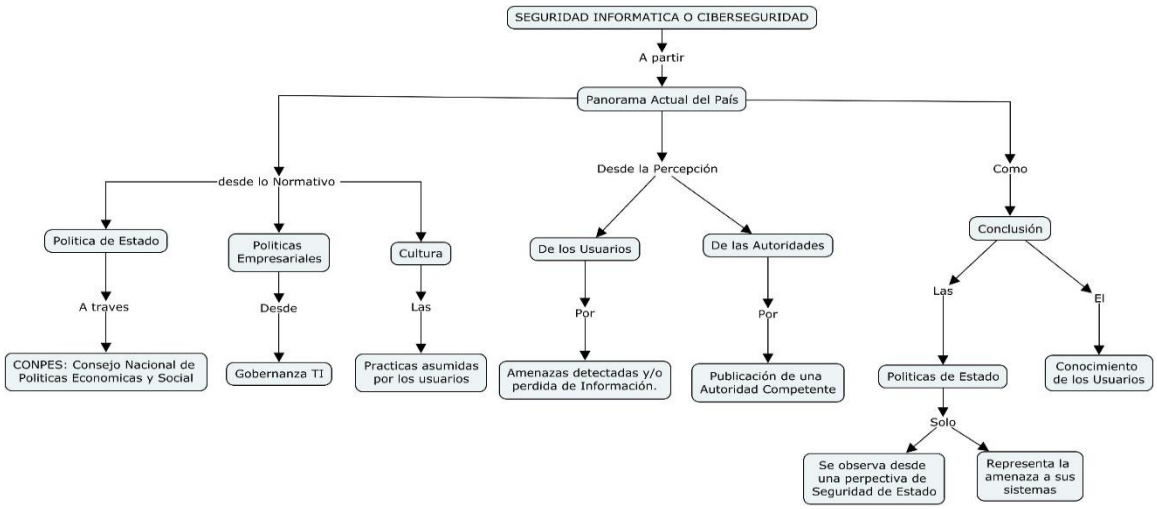
SHOSTACK Adam; (2014) Modelando Amenazas: Diseñando para Seguridad. https://www.amazon.com/Threat-Modeling-Designing-Adam-

Shostack/dp/111880998

VILLALÓN HUERTA, Antonio (2004) Códigos de buenas prácticas de seguridad. UNE/ISO/IEC 17799. Recuperado de: http://www.shutdown.es/ISO17799.pdf

Nombre y apellidos de quien elaboró este RAE	Hernando Arbey Robles Puentes
Fecha en que se elaboró este RAE	Septiembre 2018

Imagen (mapa conceptual) que resume e interconecta los principales conceptos encontrados en el texto:



Comentarios finales

Es importante los procesos de formación a todo nivel para conocer los riesgos en el que estamos sometidos quienes hacemos uso de las redes informáticas. Que hacemos transacciones de datos y muchos de ellos de gran valor.