LA SEGURIDAD EN EL CIBERESPACIO

Un desafío para Colombia

El futuro digital es de todos

MinTIC

ESCUELA SUPERIOR DE GUERRA
"General Rafael Reyes Prieto"
Colombia

La Seguridad en el Ciberespacio

Un desafío para Colombia

La Seguridad en el Ciberespacio

Un desafío para Colombia

Gladys Elena Medina Ochoa
(Editora)

Jairo Andrés Becerra
Marco Emilio Sánchez Acevedo
Carlos A. Castañeda M.
Alejandro Bohórquez - Keeney
Rafael Vicente Páez Méndez
Arístides Baldomero Contreras
Ivonne Patricia León
(Autores)

ESCUELA SUPERIOR DE GUERRA
"GENERAL RAFAEL REYES PRIETO"

MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA

BOGOTÁ D.C.

2019

LIBRO RESULTADO DE INVESTIGACIÓN

ISBN: 978-958-52165-4-9
ISBN-E: 978-958-52165-5-6

Proceso de arbitraje:
1er concepto - Evaluación: 08 de noviembre 2018
2do concepto - Evaluación: 09 de noviembre 2018

Impreso en Colombia – Printed in Colombia.

CONTENIDO

CAPÍTULO II

LA SEGURIDAD DIGITAL EN EL ENTORNO DE LA FUERZA PÚBLICA DIAGNÓSTICOS Y AMENAZAS DESDE LA GESTIÓN DEL RIESGO

CAPÍTULO III

EL IMPACTO DE LA ACADEMIA EN LA CIBERSEGURIDAD

CAPÍTULO IV

ESTADO DEL ARTE DE LA GESTIÓN DE RIESGOS EN SEGURIDAD DIGITAL EN EL SECTOR GOBIERNO EN EUROPA Y AMÉRICA DEL NORTE

CAPÍTULO V

GESTIÓN DE RIESGO EN SEGURIDAD DIGITAL EN EL SECTOR PRIVADO Y MIXTO - CONTEXTO GENERAL

AUTORES

Marco Emilio Sánchez Acevedo. Abogado colombo-español; Doctorado con mención *Cum Laude* en Tecnologías y Servicios de la Sociedad de la Información – Línea de Investigación Derecho y Tecnologías; Magister en Ciberseguridad y Ciberdefensa Nacional. Ponente en eventos académicos, autor de varias obras en la temática Derecho y tecnologías, Docente e Investigador de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto" y del área de Regulación en Ciberseguridad y Ciberdefensa Nacional.

Rafael Vicente Páez Méndez. Docente (Universidad Pompeu Fabra, Barcelona-España), actualmente, Profesor asociado (Pontificia Universidad Javeriana, Bogotá), miembro del Grupo de Investigación SiDRe. Doctor en Ingeniería Telemática con énfasis en Seguridad; Ingeniero de Sistemas con especialidad en Seguridad Informática. Investigador de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto",

Jairo Andrés Becerra. Abogado, Investigador asociado de Colciencias E, Investigador en Derecho público y TIC, con más de 15 publicaciones en el campo de las TIC y ponencias nacionales e internacionales. Docente, Investigador de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto".

Carlos A. Castañeda M. Doctor en Informática (Universidad Autónoma de Madrid), MBA (IE Business School, España). Con más de 20 años de trayectoria profesional en diversas empresas del área de Ciberseguridad y cloud computing en Colom-

bia y España, actualmente, responsable de Preventa de Soluciones de CiberSeguridad de Unisys para Latinoamérica. **(**Oficial de la Reserva Naval de Colombia en el grado de Teniente de Corbeta). Docente, Investigador de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto".

Alejandro Bohórquez - Keeney. Profesional en Política y Relaciones Internacionales (Universidad Sergio Arboleda), Magister en Inteligencia Estratégica (Escuela de Inteligencia y Contrainteligencia). Docente, Investigador de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto".

Aristides Baldomero Contreras Fernández Abogado con Especialización en Procedimiento Penal Constitucional, candidato a MBA y Máster en Supply Chain Management, Certificado en Riesgos bajo ISO31000 Risk Manager PECB. (Oficial de la Reserva Activa del Ejército Nacional). Investigador de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto".

Ivonne Patricia León. Magíster en Derecho y Politóloga (Universidad Nacional de Colombia). Experiencia en investigación, destrezas en la elaboración de trabajos escritos de carácter científico y técnico. Investigadora de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto".

PRESENTACIÓN

El presente libro, denominado "*La Seguridad en el Ciberespacio: Un desafío para Colombia",* busca presentar dentro del escenario académico e investigativo de Colombia la necesidad en primer lugar de tener como objeto de investigación el ciberespacio, como un escenario en el cual el Estado debe hacer uso de todos los medios que cuenta para preservar sus intereses y logrando proteger no solo la infraestructura critica con la que cuenta desde el campo de acción de las Fuerzas Militares sino tambien en relación a la intervención de todas las entidades público, sector académico, sector mixto privado; en pro de la búsqueda de concientización de estos nuevos riesgos latente que en campo de la ciberseguridad y ciberdefensa pueden abismarse y el impacto que pueden generar a nivel Colombia.

Los autores plantean una reflexión del nuevo estado mundial y desafíos que como país nos estamos enfrentando en los temas de ciberseguridad y ciberdefensa buscando evidenciar la importancia que todos los sectores deben asumir en pro de evaluar y mitigar los posibles riesgos a que nos enfrentamos en el tema. Desafíos que a través de una sinergia se deben manejar como Estado, buscando integrar esfuerzos desde los diferentes ámbitos como lo es las Fuerzas de Seguridad en nuevas tecnologías que se desenvuelven en las capacidades militares críticas, ante la elevada desestabilización internacional y regional producto del acceso a las nuevas tecnologías disruptivas por parte de organizaciones delincuenciales. El fortalecimiento en la educación para calificar un recurso humano especializado en el tema, generando espacios académicos e investigativos que aporten a los diferentes sectores y que sean a su vez multiplicadores en la sensibilización de los riesgos y consecuencias en el uso del internet y nuevas tecnologías, así como la entrada de la cuarta

revolución industrial espectro de amenazas a las cuales se debe responder.

Este libro resultado de investigación es producto del proyecto titulado *"Gestión de Riesgos en Seguridad Digital"* de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra realizado durante la vigencia del 2018, que a su vez hace parte de la línea de investigación 'Seguridad digital' del grupo de investigación Masa Crítica, reconocido y categorizado en (C) por Colciencias. Registrado con el código COL0123247, adscrito a la Escuela Superior de Guerra "General Rafael Reyes Prieto"

PREFACIO

Dentro de los retos que tienen las naciones hoy en día con respecto a la defensa y la seguridad nacional, se encuentran no solamente las posibles agresiones de carácter internacional, sino también de carácter interno a través del crimen organizado, que en algunas desbordan las capacidades del poder aéreo, marítimo y terrestre, sino que tienen un campo mucho más global, anónimo y letal, que es el ciberespacio al cual enfrentarse.

Colombia no es ajena a estas amenazas, por lo que nos exige revisar las estrategias que viene trabajando el país, desde la formulación del CONPES 3701 de 2011 "Lineamientos de política para la Ciberseguridad y Ciberdefensa", buscando el desarrollo de la capacidad cibernética en Colombia y el CONPES 3854 de 2016 "Política Nacional de Seguridad Digital 3854 de 2016 con una visión estratégica en la que se alienta a los distintos actores involucrados a hacer un uso responsable del entorno digital y fortalecer las capacidades para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital (conpe,2016). Es por esto por lo que la Escuela Superior de Guerra como ente formador en seguridad y defensa nacional a través de la Maestría en Ciberseguridad y Ciberdefensa, y en apoyo del Ministerio de Tecnologías de la Información y las Comunicaciones ha venido desarrollando investigaciones orientadas a establecer la situación actual de los diferentes sectores que enfrentan riesgos de seguridad digital en el ciberespacio.

El presente trabajo, producto investigación vienen explorando diferentes áreas de la Ciberseguridad y la Ciberdefensa como son el impacto de la educación en la ciberseguridad, la gestión del riesgo digital, las responsabilidades de las FFMM en la Ciberdefensa, el estado del arte sobre las capacidades en

Ciberseguridad que desarrollan algunos gobiernos entre otras.

Esta obra es un valioso instrumento teórico de consulta para el análisis de estas temáticas, donde estudiantes, profesionales e interesados en el tema de Ciberseguridad y Ciberdefensa, encontraran conceptos, y propuestas de este nuevo entorno cibernético que está impactando a múltiples actores en el ámbito de la seguridad y defensa nacional.

Mayor General JAIME AGUSTÍN CARVAJAL VILLAMIZAR
Director Escuela Superior de Guerra "General Rafaél Reyes Prieto"

INTRODUCCIÓN

LA CIBERSEGURIDAD, GESTIÓN DEL RIESGO Y LA RESILENCIA, PERSPECTIVA DE LA EVOLUCIÓN DE LA POLÍTICA PÚBLICA COLOMBIANA[1]

Carlos Castañeda Marroquí[2]
Escuela Superior de Guerra

1. LA CIBERSEGURIDAD, GESTIÓN DEL RIESGO Y LA RESILENCIA, PERSPECTIVA DE LA EVOLUCIÓN DE LA POLÍTICA PÚBLICA COLOMBIANA

La forma en que vivimos está respaldada por los sistemas de información, que permiten desarrollar nuestra vida diaria, habilitando actividades ahora tan comunes como la compra de viajes y facilitando que las empresas desarrollen sus actividades comerciales. El funcionamiento de nuestras organizaciones em-

1 Capítulo de libro resultado del proyecto de investigación titulado "Gestión de Riesgos en Seguridad Digital" de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra, que a su vez hace parte de la línea de investigación 'Desarrollo científico, tecnológico e innovación y política ambiental' del grupo de investigación 'Masa Crítica', reconocido y categorizado en (C) por Colciencias. Registrado con el código COL0123247, está adscrito a la Escuela Superior de Guerra de la República de Colombia.

2 Doctor en informática de la Universidad Autónoma de Madrid y cuenta con un MBA de IE Business School (España). Ha trabajado por más de 20 años en varias empresas en el área de ciberseguridad y cloud computing en Colombia y España. Actualmente es responsable de Preventa de Soluciones de CiberSeguridad de Unisys para Latinoamérica. Oficial de la Reserva Naval de Colombia en el grado de Teniente de Corbeta. Docente, Investigador de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra. E-mail: carlos.castanneda@gmail.com

presariales, la gestión de las cadenas de suministro y la operación del gobierno depende de los flujos seguros de información.

La información tiene gran valor, es por ello que a medida que los ataques cibernéticos crecen en número y sofisticación, la amenaza se percibe cada vez más como un problema tanto en el contexto de Seguridad Nacional como en el internacional. Sin embargo, las evaluaciones de cuán real es la amenaza, dónde radica el peligro, quién es el más adecuado para responder a ella y qué tipo de medidas y estrategias son apropiadas para proteger a las sociedades de la información contra los actores malintencionados más cuál debiese ser la mejor forma de salvaguardar la estabilidad a largo plazo varían ampliamente.

Todo esto hace que nuestras sociedades, nuestras organizaciones y nosotros mismos seamos vulnerables a innumerables amenazas de capitalización. En un entorno organizacional, la Seguridad de la información es un proceso interminable de protección de la información y los sistemas de información que la producen. Teniendo en cuenta los posibles efectos de una falla en esta protección, la Seguridad de la información protege los principales activos financieros y de otro tipo de la organización. Los activos no financieros, como la marca, la reputación y las relaciones con los clientes, socios y proveedores, pueden sufrir graves daños en caso de que se produzca tal falla. Así, hablando claramente, la Seguridad de la información hoy protege la capacidad de una organización para funcionar.

Por su parte, los sistemas de información modernos exhiben un diseño característicamente dinámico, y la amplia disponibilidad de tecnologías asociadas crea un terreno fértil, no solo para comportamientos no anticipados (errores), sino también para actores maliciosos innovadores que buscan y explotan nuevos modos de falla y vectores de ataque. Para agravar estos problemas, la información personal, financiera y de Seguridad de la actualidad tiene un valor intrínseco tal, que la pérdida, la des-

viación o la alteración pueden producir rápidamente consecuencias imprevistas. Los modos de peligro, las probabilidades y las consecuencias están mal caracterizados y cambian rápidamente.

Los Estados son cada vez más conscientes de la necesidad de abordar seriamente los enormes desafíos de proteger sus redes de información, especialmente las relacionadas con la Seguridad Nacional y las infraestructuras críticas de cualquier atacante. Las estrategias plasmadas en políticas públicas han demostrado que hay más firmeza en la visión de largo plazo que responder preguntas técnicas. La cuestión de la Seguridad cibernética debe ubicarse dentro de un marco más amplio de cooperación, normas y reglas para un comportamiento estatal apropiado y responsable que garantice el uso correcto del ciberespacio.

Las preocupaciones surgen de un mundo cada vez más interconectado, donde los sistemas de infraestructura dependen de nuevas tecnologías que, al tiempo que expanden los servicios y promueven la maduración y el crecimiento del sistema, exponen dichos sistemas a nuevos y en cascada riesgos que podrían devastar el funcionamiento normal de sistemas importantes.

Dichos riesgos, que van desde la Ciberseguridad hasta la pérdida de la biodiversidad y los importantes servicios ecosistémicos, representan desafíos crecientes para los gestores de riesgos en el siglo XXI. Requieren el desarrollo de estrategias convencionales de Gestión de Riesgos, pero también estrategias impulsadas por la resiliencia para proteger adecuadamente contra las consecuencias indeseables de eventos inciertos, inesperados y a menudo dramáticos.

Además de las infracciones de datos y los impactos financieros directamente asociados, los ciberataques pueden comprometer la Infraestructura Crítica, como los servicios públicos, las comunicaciones, los sistemas financieros e incluso los sistemas

de transporte. El alto nivel de conectividad y dependencia de los sistemas de información para las operaciones y la gestión de los servicios de Infraestructura Crítica puede tener la consecuencia de fallas generalizadas que involucran Dependencias dentro y entre múltiples sectores económicos.

A medida que las sociedades experimentan la transformación digital, las apuestas por la Ciberseguridad han aumentado. Los gobiernos y los organismos reguladores están desarrollando nuevas leyes de cumplimiento destinados a impulsar mejoras de la Ciberseguridad en las organizaciones. Es por ello que el enfoque de la Ciberseguridad entendida como una acción reactiva, es limitado. Por ello la construcción de una ciberestrategia debe basarse en un enfoque más amplio que incluya la Gestión de Riesgos, un marco de referencia de seguridad (NIST, ISO 27000, ISO 30000, etc.) y el cumplimiento normativo. Si bien estos enfoques proporcionan una guía importante para desarrollar una Estrategia de Seguridad, son solo un comienzo.

Se entiende como riesgo la posibilidad genérica de pérdida o lesión y la Gestión del Riesgo como una disciplina que busca optimizar las decisiones sobre medidas de protección, buscando maximizar el valor esperado frente a los riesgos conocidos, basada en datos históricos. Actualmente esta visión se ve complementada a través del término de resiliencia como la capacidad de que tiene un sistema de tolerar y recuperarse ante un desastre.

El significado de resiliencia, seguridad y Gestión del Riesgo, sus significados en el contexto de la Ciberseguridad están interrelacionadas (Christou, 2016; Eisenberg, Linkov, Park, Bates, Fox-Lent, & Seager, 2014). El siguiente diagrama proporciona la relación entre la Ciberseguridad, la Seguridad de la información, la Gestión de Riesgos y la resiliencia.

Figura 1. Relación entre los conceptos de Seguridad Digital.
Fuente: Elaboración propia a partir de la información analizada

La *Directiva de Política Presidencial de los Estados Unidos* distingue entre Seguridad y la capacidad de recuperación, reiterando la necesidad de "prepararse y adaptarse a las condiciones cambiantes y resistir y recuperarse rápidamente de las interrupciones" (Eisenberg, Linkov, et.al. 2014). La Gestión del Riesgo de Ciberseguridad permite evaluar la probabilidad en un gran conjunto de posibles ataques, y determinar cuánto invertir con el tiempo en diseños de protección y medidas o en resiliencia y respuesta y recuperación rápidas. El proceso de Gestión de Riesgos implica seleccionar entre varias alternativas con diversos costos y beneficios a fin de reducir el riesgo restante a un nivel aceptable. Definir este umbral de riesgo y seleccionar entre alternativas no es un ejercicio sencillo.

La visión sobre la resiliencia como una alternativa se hace cada vez más sólida. Muchos han adoptado las cinco funciones simultáneas y continuas del NIST (Wendt, 1992), estas brindan una visión estratégica de alto nivel del ciclo de vida de la Gestión del Riesgo de Ciberseguridad de una organización.

Así, teniendo esto en cuenta, se puede apreciar la evolución de la política pública colombiana entre el *Conpes 3701* y el *Conpes 3158*, donde se ha utilizado el concepto de resiliencia para evaluar la capacidad de mantener la Seguridad y la flexibilidad y para recuperarse de una serie de posibles eventos adversos. Además, la capacidad de recuperación ofrece la capacidad de revisar mejor cómo los sistemas pueden ajustarse continuamente a la información, las relaciones, los objetivos, las amenazas y otros factores cambiantes para adaptarse frente al cambio, particularmente aquellos cambios potenciales que podrían arrojar resultados negativos.

Las diferencias conceptuales entre el análisis de riesgo y el análisis de resiliencia se comprenden y desarrollan debido a la atención relativamente reciente a la resiliencia. La cuantificación de la resiliencia es menos madura que su metodología de pares en la evaluación de riesgos tradicional, que de otra manera tiene décadas de uso práctico. Esto se debe a que la resiliencia es particularmente relevante para lidiar con amenazas inciertas, que son siempre difíciles, si no imposibles, de cuantificar.

2. LA CIBERSEGURIDAD COMO PRIORIDAD EN EL CONTEXTO GEOPOLÍTICO.

A través de la teoría de las relaciones internacionales, el constructivismo comprende al sistema internacional como un ente que responde a una seguridad colectiva (Wendt, 1992). Los Estados tienen perspectivas similares sobre Ciberseguridad que funcionan para proteger Internet al bloquear actividades que influyen negativamente en la Seguridad del Estado, la economía y las actividades financieras personales. Sin embargo, las diferencias tradicionales, institucionales y culturales hacen que los Estados usen diferentes estrategias. Los Estados intentan resolver cuestiones sobre la aplicación de las leyes y normas internacionales, ya que todavía no existe un entendimiento multilateral

sobre cómo aplicarlas al ámbito de la Ciberseguridad o incluso sobre por qué hacerlo es importante para el futuro.

De ahí la importancia de garantizar la disponibilidad y la pluralidad de Internet a través de la cooperación internacional. Las infraestructuras de Internet han brindado una gran cantidad de oportunidades a la comunidad mundial al facilitar el comercio y la comunicación. El ciberespacio ha sido una red mundial abierta que ha reforzado la educación, la innovación tecnológica y el intercambio de conocimientos e ideas. Este espacio de libertad, desarrollo personal y progreso económico garantiza protección.

Debido a que las infraestructuras de Internet e informática cruzan las fronteras y los sistemas legales nacionales por igual, casi todos los Estados tienen un interés vital en garantizar su resiliencia, Seguridad y estabilidad por razones económicas, así como por la Seguridad ciudadana. Los principios generales para el ciberespacio, como el uso pacífico, la obligación de asegurar las infraestructuras críticas, la cooperación entre los Estados para la atribución de ataques cibernéticos y la reciprocidad en aspectos que garanticen la persecución del delito son agenda entre varios Estados.

Surge entonces la importancia de evaluar la creación de un consenso internacional compartido sobre las normas de conducta en el ciberespacio. De acuerdo con la Estrategia Internacional para el Ciberespacio, que fue elaborada por los Estados Unidos (Clinton, 2011), los entendimientos y normas compartidos deberían centrarse en los mundos físico y cibernético por igual. Estos deben incluir las libertades fundamentales en línea y fuera de línea, los derechos de propiedad, la privacidad pública, la protección contra el delito cibernético, el derecho a la legítima defensa, la estabilidad técnica, el acceso confiable y la resiliencia nacional.

Internet es un nuevo ámbito de confrontación política y la comunidad mundial aún no está cien por cien preparada para

combatir las amenazas a la Seguridad de la información. Los Estados intentan ir a la velocidad de los cambios tecnológicos administrando el ciberespacio en su territorio de acuerdo con las leyes nacionales permitiendo a sus ciudadanos las libertades y derechos fundamentales para su uso (Kittichaisaree, 2017).

La Unión Europea para luchar contra el delito cibernético, basa su visión en poder construir la solidaridad y establecer una cooperación política entre los países miembros. Un código de conducta es necesario para garantizar la libertad de expresión y la fiabilidad de Internet. La Declaración de Deauville del G8 de diciembre de 2011 (Christou, 2016), acordó una serie de principios sobre cómo garantizar la fortaleza continua de Internet como recurso para la sociedad global: libertad, gobierno de múltiples partes interesadas, respeto a la privacidad y propiedad intelectual, Ciberseguridad y protección contra el cibercrimen.

Los responsables de la formulación de políticas deben desarrollar un papel para garantizar una recopilación coherente de datos de incidentes relevantes. La divulgación de información podría ayudar a controlar el verdadero alcance de las amenazas ya que el control específico del ciberespacio es difícil pues los Estados al no tener monopolios, advierten que la responsabilidad es difícil de atribuir. Para ello, la diplomacia en la Ciberseguridad debe buscar la cooperación internacional para luchar contra las amenazas cibernéticas mediante el desarrollo de acuerdos sobre lo que constituye una actividad cibernética responsable por parte de los Estados.

Este proceso, se está gestando para conciliar los diferentes conceptos existentes sobre lo que podría ser el comportamiento estatal legítimo: algunos se centran en la importancia de la idea de que los "bienes comunes globales" se mantengan libres de ciberataques, mientras que otros ven la ciberesfera como otro dominio para la guerra. El fomento de la confianza

como un medio de respuesta a los riesgos de la percepción errónea y la escalada, que se ven incrementados por los atributos característicos del ciberespacio, como su dinamismo y anonimato intrínsecos. Por lo tanto, las transparencias podrían crear la base de confianza entre la comunidad estatal que es necesaria para que los Estados puedan celebrar acuerdos legalmente vinculantes.

Los derechos y responsabilidades del Estado en el ciberespacio (Shackelford, & Andres, 2010), pueden realizarse tanto en el ámbito político como en el jurídico y los Estados ya comienzan a abordar políticamente la responsabilidad del Estado. Esta comprensión de las responsabilidades políticas y legales de los Estados pueden ayudar a establecer el Derecho Internacional, los Estados tienen una obligación legal, así como una responsabilidad política de trabajar más rápido hacia la creación de ellos para el ciberespacio, ya que el proceso es actualmente muy lento. El desarrollo de mecanismos de cooperación en materia de delito cibernético entre los Estados Unidos, China y Rusia constituye una base para construir normas dirigidas a un comportamiento estatal responsable con relación a los aspectos militares del dominio cibernético. Por último, es importante la regulación internacional en el ámbito cibernético. Si bien no se ha cuestionado la necesidad de cooperación internacional y leyes públicas que regulen la respuesta a los desafíos y ataques que se originan en el ciberespacio, es difícil determinar cómo se puede aplicar la ley existente al ámbito cibernético.

Este capítulo sirve de introducción general a los conceptos y aplicación de las diferentes aproximaciones en el ámbito de la Ciberseguridad en diferentes países y escenarios que se desarrollarán en el libro, específicamente en lo que se refiere a la Gestión de Riesgos. Los siguientes capítulos describen las aplicaciones de la resiliencia a la Infraestructura Crítica desde varias perspectivas metodológicas y analíticas.

CAPÍTULO 1

LA CIBERSEGURIDAD Y LA CIBERDEFENSA, LA NECESIDAD DE GENERAR ESTRATEGIAS DE INVESTIGACIÓN SOBRE LAS TEMÁTICAS QUE AFECTAN LA SEGURIDAD Y DEFENSA DEL ESTADO[3]

Marco Emilio Sánchez Acevedo[4]
Escuela Superior de Guerra

1. LA INVESTIGACIÓN COMO ELEMENTO ESENCIAL DE LA POLÍTICA DE SEGURIDAD DIGITAL EN COLOMBIA.

1.1 La política de Seguridad Digital colombiana – estructuración desde el entendimiento gráfico.

Es pertinente abordar como punto inicial, el objetivo general del contenido en el (numeral 5.1.) del documento *Conpes de Seguridad Digital 3854 de 2016*, en el que se señala como tal el "[…] fortalecer las capacidades de las múltiples partes

3 Capítulo de libro resultado del proyecto de investigación titulado "Gestión de Riesgos en Seguridad Digital" de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra, que a su vez hace parte de la línea de investigación 'Desarrollo científico, tecnológico e innovación y política ambiental' del grupo de investigación 'Masa Crítica', reconocido y categorizado en (C) por Colciencias. Registrado con el código COL0123247, está adscrito a la Escuela Superior de Guerra de la República de Colombia

4 Abogado colombo-español; Doctorado con mención Cum Laude en Tecnologías y Servicios de la Sociedad de la Información – Línea de Investigación Derecho y Tecnologías; Magister en Ciberseguridad y Ciberdefensa Nacional. Ponente en eventos académicos, autor de varias obras en la temática Derecho y tecnologías, Docente e Investigador de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto" y del área de Regulación en Ciberseguridad y Ciberdefensa Nacional.

interesadas para identificar, gestionar, tratar y mitigar los riesgos de Seguridad Digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia […]". En este sentido, la Política Nacional que se genera, parte de la aceptación de las recomendaciones dadas por la OCDE a fin que se creen condiciones para la participación de las múltiples partes interesadas, en palabras de la OCDE:

> […] (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 (OCDE, 2015),

Tal y como se ha señalado en investigaciones anteriores[5], el documento *Conpes de Seguridad Digital* establece que es necesario reforzar las capacidades de Ciberseguridad con un enfoque de Gestión de Riesgos, así como reforzar las de Ciberdefensa bajo este mismo; también se determina que los esfuerzos de cooperación, colaboración y asistencia, nacionales e internacionales, relacionados con la Seguridad Digital, son insuficientes y desarticulados. Ante este panorama se plantea una nueva política, cuyo objetivo general es:

> [...] identificar, gestionar, tratar y mitigar los riesgos de Seguridad Digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía di-

5 Véase Sánchez Acevedo, M.E. (2018). Estrategia Jurídica para la Gestión, Análisis y Ciberseguridad de la Información en la Investigación Penal. *Tesis de maestría*. Bogotá: Escuela Superior de Guerra "General Rafael Reyes Prieto".

> gital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país (Conpes, 2016, p 47)

Es precisamente por ello que la política trazada por el documento *Conpes 3854 de 2016* está determinada de la siguiente manera.

Figura 2. Política trazada por el documento Conpes 3854 de 2016

Fuente: Elaboración Propia a partir del documento CONPES 3854 de 2016

Las cinco dimensiones estratégicas sobre las que se adopta el enfoque que garantice la Seguridad Digital desde la participación de las múltiples partes interesadas se define de la siguiente manera gráfica para mayor comprensión.

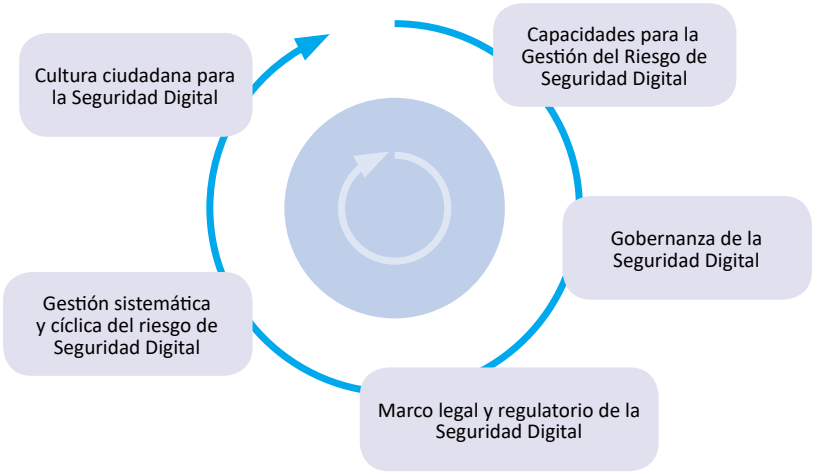


Figura 3. Las cinco dimensiones estratégicas del documento Conpes 3854 de 2016
Fuente: Elaboración propia partir del documento CONPES 3854 de 2016

Estas dimensiones estratégicas han establecido un conjunto de acciones tendientes al desarrollo en los siguientes términos:

a. **Dimensión estratégica 1. Establecer un marco institucional para la Seguridad Digital consistente con un enfoque de Gestión de Riesgos.**

Entre los elementos destacables del documento Conpes en referencia está la creación de la figura de coordinador nacional de Seguridad Digital, el cual tendrá entre sus funciones:

> Dirigir la implementación de la política nacional de Seguridad Digital y hacer seguimiento continuo de la misma; llevar a cabo la coordinación interinstitucional e intersectorial en temas de Seguridad Digital; garantizar que el alcance de la Seguridad Digital en el país incluya la prosperidad económica y social; así como la Ciberseguridad, para enfrentar nuevos tipos de crimen, delincuencia, y otros fenómenos que afecten la seguridad nacional; y la Ciberdefensa [...] (Conpes, 2016, p. 50)

De igual modo este coordinador debe propender por:

> Garantizar que los programas, proyectos y campañas de concientización y sensibilización, así como las capacitaciones que adelanten las diferentes entidades, se diseñen a partir de los lineamientos y orientaciones que emita la Comisión Nacional Digital y de Información Estatal, o de quien haga sus veces, con el fin de evitar la duplicación de esfuerzos y garantizar la eficiencia en el manejo de los recursos; recomendar nuevas acciones en colaboración con las múltiples partes interesadas, en vista de la rápida tasa de desarrollo de la tecnología y los escenarios de ataques cibernéticos; coordinar con la comisión Nacional Digital y de Información Estatal, y con las múltiples partes interesadas, los informes respecto del cumplimiento de los lineamientos de orientación superior establecidos para la implementación de la política nacional de Seguridad Digital en el marco de sus principios fundamentales (Conpes, 2016, p 50).

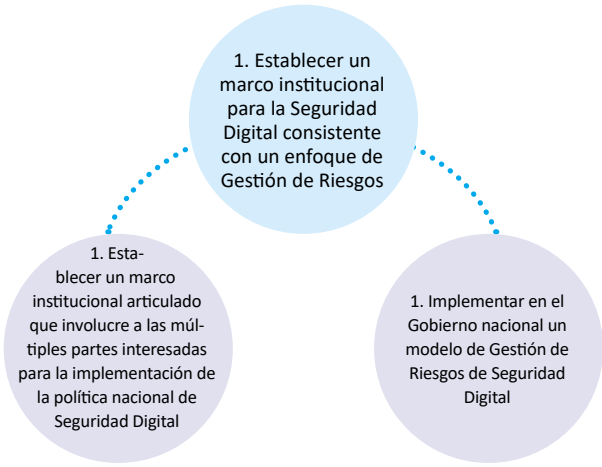


Figura 4 a. Dimensión estratégica 1. Establecer un marco institucional para la Seguridad Digital consistente con un enfoque de Gestión de Riesgos.

Fuente: Elaboración propia adoptada del CONPES 3854 de 2016

a. **Dimensión estratégica 2. Crear 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.**

Dentro de los elementos estratégicos que se deben resaltar al respecto, se encuentran los concernientes al establecimiento de mecanismos de participación activa y permanente de las múltiples partes interesadas en la Gestión del Riesgo de Seguridad Digital; la adecuación del marco legal y regulatorio en torno a la dinámica de la economía digital y sus incertidumbres inherentes; la identificación y abordaje de los posibles impactos negativos que otras políticas pueden generar sobre las actividades de las múltiples partes interesadas o sobre la prosperidad económica y social en el entorno digital, y la generación de confianza a las múltiples partes interesadas en el uso del entorno digital; por último la promoción de comportamientos responsables en el entorno digital (Conpes, 2016, p 48)

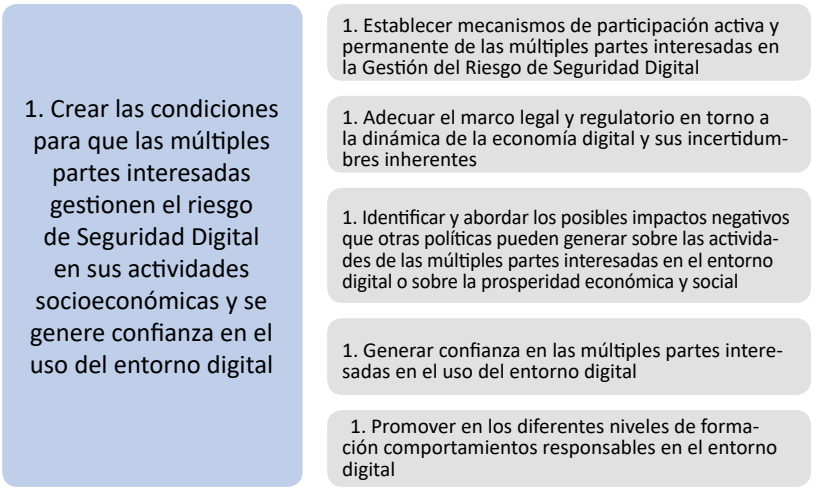


Figura 5 b. Dimensión estratégica 2. Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de Seguridad Digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital.

Fuente: Elaboración propia a partir del CONEPS 3854 del 2016

b. *Dimensión estratégica 3. Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y trasnacional, con un enfoque de Gestión de Riesgos.*

Es necesario empoderar a los ciudadanos y al Estado con relación a los riesgos del entorno digital, y consolidar las capacidades del país para hacer frente al crimen, la delincuencia y otros fenómenos que afectan la Seguridad Nacional en este espacio. Para esto es imperativo

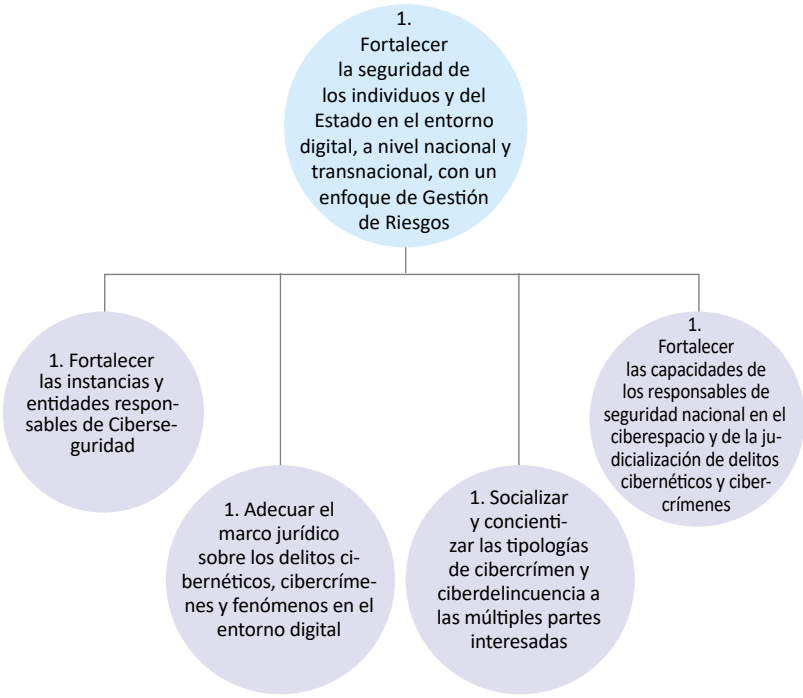


Figura 6 c. Dimensión estratégica 3. Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y trasnacional, con un enfoque de Gestión de Riesgos.

Fuente. Elaboración propia adaptada del documento *Conpes 3854 de 2016*

fortalecer a las entidades responsables de Ciberseguridad; adecuar el marco jurídico referente a los cibercrímenes y ciber-

delincuencia, así como socializar y concientizar acerca de estos a las múltiples partes interesadas; también hay que fortalecer las capacidades de los responsables de seguridad nacional en el ciberespacio y la de judicialización de este tipo de conductas.

c. *Dimensión estratégica 4. Fortalecer la Defensa y soberanía nacional en el entorno digital con un enfoque de Gestión de Riesgos.*

Es fundamental desarrollar capacidades de prevención, detección, contención, respuesta, recuperación y Defensa para garantizar los fines del Estado, así como mejorar la protección, preservar la integridad y la resiliencia de la Infraestructura Crítica Cibernética Nacional; para lo cual es necesario fortalecer las instancias y entidades responsables de la Defensa Nacional en el entorno digital, adecuar el marco jurídico para abordar la protección y Defensa del mismo; generar una Estrategia de Protección y Defensa de la Infraestructura Crítica Cibernética Nacional, fortalecer el esquema de identificación, prevención y gestión de incidentes digitales, con la participación activa de las múltiples partes interesadas, y fortalecer las capacidades de los responsables de garantizar la Defensa Nacional en el entorno digital.

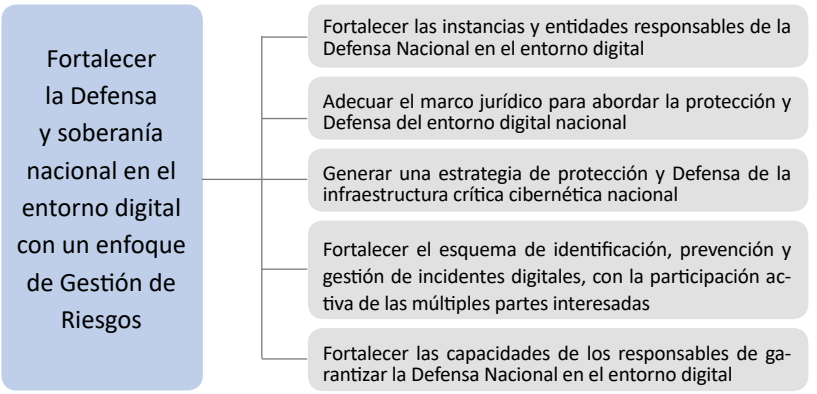


Figura 7 d. Dimensión estratégica 4. Fortalecer la Defensa y soberanía nacional en el entorno digital con un enfoque de Gestión de Riesgos

Fuente: Elaboración propia adaptada del documento Conpes 3854 de 2016

d. *Dimensión estratégica 5. Generar mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia en Seguridad Digital, a nivel nacional e internacional.*

La cooperación nacional entre las múltiples partes interesadas y la cooperación internacional en materia de Seguridad Digital resultan ser esenciales, para ello se deben generar mecanismos para impulsarlas, así como fortalecer la cooperación, colaboración y asistencia entre bloques de países.

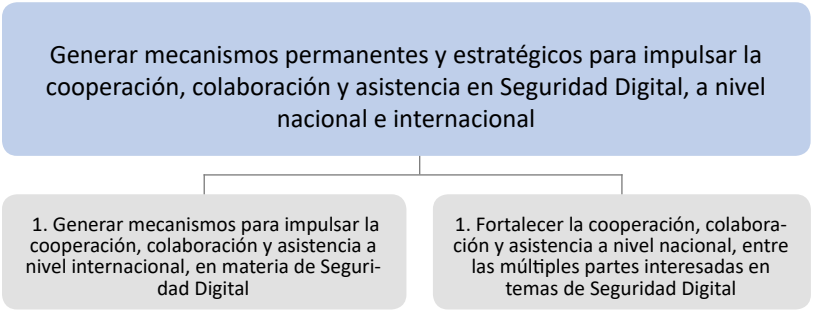


Figura 8 e. Dimensión estratégica 5. Generar mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia en Seguridad Digital, a nivel nacional e internacional

Fuente: Elaboración propia adaptada del documento Conpes 3854 de 2016

1.2. Conceptualización.

1.2.1. *Ciberseguridad.*

Para abordar la Ciberseguridad y Ciberdefensa debemos señalar el concepto de ciberespacio, entendiéndose por este el espacio artificial creado por el conjunto de sistemas de la información y telecomunicaciones que utilizan las TIC, es decir de redes de ordenadores, mucho más que Internet, más que los mismos sistemas y equipos, el *hardware* y el *software* e incluso que los propios usuarios, es un nuevo espacio, con sus propias leyes físicas que, a diferencia de los demás, ha sido

creado por el hombre para su servicio (Min. Defensa España y IEEE, 2012).

> El ciberespacio es la dimensión generada durante el tiempo de interconexión e interoperabilidad de redes, sistemas, equipos y personal relacionados con los sistemas informáticos cualesquiera sean estos y las telecomunicaciones que los vinculan. (CARI, 2013, p. 4)

La *Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009* que resuelve adicionar al *Artículo 1.8* de la *Resolución CRT 1740 de 2007*, algunas definiciones y aunque a pesar de que estas disposiciones han sido derogadas, los conceptos siguen vigentes en la actualidad entre ellos:

> [...] **Ciberseguridad:** el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de Gestión de Riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. La Ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos y usuarios contra los riesgos de seguridad correspondientes en el ciberentorno […] **Ciberespacio:** es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. […]

La Asociación de Auditoría y Control sobre los Sistemas de Información —*Information Systems Audit and Control Association* (en adelante: Isaca)— define la Ciberseguridad como "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada,

almacenada y transportada por los sistemas de información que se encuentran interconectados" (Audea.com, 2016, párr. 3).

Para S. Koch (2015, p. 89) la Ciberseguridad "[…] se entiende que es la situación de ausencia de amenazas realizadas por medio de, o dirigidas a las tecnologías de la comunicación y de la información y a sus redes".[6]

Adicionalmente, debemos comprender qué es seguridad de la información. Entendida esta como la preservación de la confidencialidad, integridad y disponibilidad de la información, donde confidencialidad se entiende como una propiedad, a saber, que la información no sea puesta a disposición de otros sin autorización; integridad, por su parte, es la propiedad de mantener la exactitud y *completitud* de la información; y disponibilidad es la propiedad de que la información sea accesible y utilizable ante el requerimiento de una entidad autorizada (Kosutic, 2012).

En palabras de la Unión Internacional de Telecomunicaciones (en adelante: UIT), se puede definir así:

> El objetivo de la Ciberseguridad es contribuir a la preservación de las fuerzas y medios organizativos, humanos, financieros, tecnológicos e informativos, adquiridos por las instituciones, para realizar sus objetivos. La finalidad de la seguridad informática es conseguir que ningún perjuicio pueda poner en peligro su perpetuidad. Para ello se tratará de reducir la probabilidad de materialización de las amenazas; limitando los daños o averías resultantes; y logrando que se

6 Tomado de la *Revista Ensayos Militares*, artículo titulado "La libertad en el ciberespacio: Ciberseguridad y el principio del daño" por Sebastián Koch, p. 89, volumen 1 N° 2 noviembre de 2015, versión en línea

> reanuden las operaciones normales tras un incidente de seguridad, en un plazo de tiempo razonable y a un coste aceptable. (UIT, 2007, p. 5)
>
> Así mismo el documento *Conpes 3854 de 2016* señala que:
>
> [...] Seguridad Digital: es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la Gestión del Riesgo de Seguridad Digital; (ii) la implementación efectiva de medidas de Ciberseguridad; y (iii) el uso efectivo de las capacidades de Ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.

Así las cosas, Ciberseguridad es la Seguridad de la información en el ciberespacio; en otras palabras, cuando se busca proteger la información contenida en el *hardware*, redes, *software*, infraestructura tecnológica o servicios, nos encontramos en el ámbito de la Seguridad informática o *Ciberseguridad* (Audea.com, 2016).

1.2.2. *Ciberdefensa.*

Los Estados organizan la Defensa de la Seguridad mediante el establecimiento de una Estrategia Nacional; de acuerdo con las amenazas y los consiguientes riesgos se planean y definen unas estrategias de Defensa abordando diferentes frentes como el territorial, aéreo, fronterizo, económico y el del ciberespacio, razón por la cual tiene que existir una Ciberdefensa que garantice la Ciberseguridad (Min. Defensa España, IEEE, 2012).

Ciberdefensa es, entonces, el conjunto de acciones u operaciones activas o pasivas desarrolladas en el ámbito de las redes,

sistemas, equipos, enlaces y personal de los recursos informáticos y teleinformáticos de la Defensa a fin de asegurar el cumplimiento de las misiones o servicios para los que fueran concebidos, a la vez que se impide que Fuerzas enemigas los utilicen para cumplir los suyos.

Se ha planteado que el proceso de la Ciberdefensa inicia por la Inteligencia informática con el ciberespacio como ambiente, para poder obtener los elementos descriptores de los escenarios que permitan parametrizar las amenazas y dimensionar los riesgos, para así posibilitar el diseño de los instrumentos de Defensa (CARI, 2013).

La Ciberdefensa se efectúa en términos de la Defensa activa y pasiva del centro de operaciones y los medios de información que posee la institución con el fin de resistir los ataques cibernéticos que sufra la entidad, cuya arma rectora son las comunicaciones militares que coadyuvan en la protección cibernética de la Infraestructura Crítica del país. Lo anterior en el ámbito de lo dispuesto por las Fuerzas Militares de Colombia (FF. MM. y Ejército Nacional, 2015).

> A partir de lo mencionado, (la defensa activa es una) estrategia determinada en adquirir una capacidad de defensa del ciberespacio, combinando la protección interior de los sistemas, la vigilancia permanente de redes sensibles y la respuesta rápida en caso de ataque, contrarrestando las amenazas ciberespaciales y garantizando acceso al ciberespacio; (y la defensa pasiva es) la estrategia para la protección de los activos relacionados con los sistemas de información a través de controles detectivos, correctivos, disuasivos que contrarresten las posibles amenazas (FF. MM. y Ejército Nacional, 2015, p 5).

En este punto es importante reseñar que en el país se cuenta con el Grupo de Respuesta a Emergencias Cibernéticas de

Colombia (en adelante: Colcert), el cual tiene como responsabilidad central la coordinación nacional de la Ciberseguridad y Ciberdefensa, la cual estará enmarcada dentro del proceso misional de gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional.

Su propósito principal es la coordinación de las acciones necesarias para la protección de la Infraestructura Crítica del Estado colombiano frente a emergencias de Ciberseguridad (Colcert, 2013).

De acuerdo con Colcert, el CSIRT de la Policía Nacional de Colombia registró menos incidentes cibernéticos en 2012 que en 2011; esto lo ubica, junto con Chile, como uno de los pocos países latinoamericanos con esa distinción.

No obstante, no es claro si esto se debió a una reducción real en el número de incidentes o a una mejor gestión de la Seguridad por parte de las agencias gubernamentales atendidas por estos equipos nacionales de respuesta a incidentes de Seguridad cibernética, como son los CSIRT, o a la implementación de políticas que cambiaron la cobertura de la asistencia prestada por los equipos de respuesta de Colombia (OEA, 2013).

También está el Sistema de Información del Centro de Operaciones del Ejército Nacional (en adelante: SICOE); mediante esta herramienta las Unidades operativas mayores y menores del Ejército reportan todos y cada uno de los eventos y situaciones operacionales que se presentan en todo el territorio nacional.

Su objetivo primordial consiste en promover la información en el momento requerido, permitiendo realizar análisis cuantitativos y cualitativos de cualquier situación operacional bajo los niveles de Seguridad que garanticen la integridad y la reserva de la información (OEA, 2013).

Además, está el Sistema de Información Geográfica del Ejército (en adelante: SIGE), esta herramienta ha sido diseñada para la captura, almacenamiento, manipulación, análisis, modelación y presentación de datos militares referenciados; el SIGE brinda información geográfica detallada para facilitar el proceso militar en todas las decisiones y es direccionado desde el Comando Conjunto Cibernético (en adelante: CCOC), (FF. MM. y Ejército Nacional, 2015).

1.3. La incorporación de la Ciberseguridad en la Política Nacional desde el entendimiento de la Política Internacional.

Es del caso hacer una referencia de cómo los distintos Estados han adoptado e incorporado el concepto de Ciberseguridad desde la política tal como en adelante se describe.

La primera referencia es la Estrategia de Ciberseguridad Europea, nacida como un conjunto de acciones encaminadas a solventar y mejorar el espacio en la red. El documento nació arropado por una serie de órganos, instituciones y políticas que ya se habían estado trabajando alrededor de las diversas dimensiones de la Seguridad desde finales de 1990 (Machín y Gazapo, 2016). La Estrategia de Ciberseguridad de la Unión Europea establece los planes para prevenir y responder a las perturbaciones y ataques que pudieran afectar a los sistemas de telecomunicaciones de este bloque de países. La UE tiene, en este contexto, una extraordinaria importancia, no solo porque agrupa a 28 países industrializados -que en la economía digital mundial juegan un papel relevante-, sino que en ellos las tecnologías digitales son el paradigma sobre la economía y la sociedad en su conjunto, mucho más que en otro lugar.

Además, en el Viejo Continente proporcionalmente están más amenazados que en otras partes; como se ha visto con los crecientes ciberataques dirigidos por bandas internacionales co-

nectadas entre sí y que operan con un elevado nivel técnico. Ante esta perspectiva, la ciberdelincuencia nos lleva a una cruda realidad en países abiertos e interconectados como los de la UE (de Carlos Izquierdo, 2016).

En cuanto a lo mencionado, cabe traer a colación la más reciente Directiva del Parlamento Europeo y del Consejo de la UE encaminada a determinar las medidas para garantizar un elevado nivel común de seguridad de las redes y sistemas de información, a fin de mejorar el funcionamiento del mercado interior, (PE y Consejo, 2016, p. 1). Esta contiene las siguientes prerrogativas:

> [...] a) Establece obligaciones para todos los Estados miembros de adoptar una Estrategia Nacional de Seguridad de las redes y sistemas de información; b) Crea un Grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar la confianza y seguridad entre ellos; c) Crea una red de equipos de respuesta a incidentes de seguridad informática a (en lo sucesivo, «red de CSIRT», por sus siglas en inglés de «computer security incident response teams») con el fin de contribuir al desarrollo de la confianza y seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz; d) Establece requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales; e) Establece obligaciones para que los Estados miembros designen autoridades nacionales competentes, puntos de contacto únicos y CSIRT con funciones relacionadas con la seguridad de las redes y sistemas de información. (PE y Consejo, 2016, pp. 11 - 12)

Esta regulación establece las reglas de Seguridad cibernética (o conjuntos de controles de Seguridad) para las empresas

que suministran servicios a la sociedad que se han categorizado como esenciales (OEA 2018). Allí se establecen un conjunto de sectores, referenciados como estratégicos para las actividades sociales y económicas de la Unión Europea. Se relacionan el sector de la energía, de los transportes, el sector financiero, el de los servicios de agua y salud, motores de búsqueda, operadores de servicios digitales, entre otros. Así mismo, se establece la obligación de los Estados para determinar y delimitar de manera clara quiénes, de las organizaciones públicas o privadas de cada uno de los miembros son operadores de servicios esenciales.

La Estrategia china en la *Ley Nacional de Seguridad Cibernética* adoptada por el Parlamento chino en noviembre de 2016, que entró plenamente en vigencia el 31 de diciembre de 2017, establece a lo largo de siete capítulos y 79 artículos, los compromisos más importantes de las agencias del Estado, así como de quienes prestan servicios de Internet y por último de los usuarios de este. De forma inicial se establece la obligación frente a la adopción, por parte de las compañías para garantizar que Internet funcione, y para ello le obliga a la adopción de medidas técnicas y humanas, dar frente a los incidentes de Seguridad y la prevención de actividades en el ciberespacio. La política establece un régimen de vigilancia, inspección y auditoría, para garantizar la reducción de riesgos.

Estados Unidos, si bien no ha adoptado un esquema regulatorio claro, sí ha hecho un llamado para que las organizaciones y la industria adopten los estándares, metodologías, procedimientos y procesos, que garanticen la Seguridad de la información, a partir los enfoques políticos, de negocios y de tecnología del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) para abordar los riesgos cibernéticos. En el año 2014 fue publicado el marco para mejorar la Seguridad cibernética de Infraestructura Crítica que ayuda a las organizaciones a evaluar, administrar y responder al riesgo de Seguridad cibernética. Sin embargo, ataques como WannaCry y NotPetya han demostrado que ello no es suficiente.

Luego de la Cumbre Mundial sobre la Sociedad de la Información del año 2003, un conjunto de 170 países determinó la necesidad de que se pudiera beneficiar de las oportunidades de las TIC para acceder a la infraestructura, a la información y al conocimiento, la seguridad en el uso de las TIC; desarrollo y ampliación de aplicaciones TIC; y alentar la cooperación internacional y regional (World Summit on the Information Society, 2003).

Precisamente por ello, en 2004, la OEA, a través del Comité Interamericano contra el Terrorismo (CICTE), y su Programa de Seguridad Cibernética, inició el desarrollo de su agenda. La Organización de Estados Americanos (en adelante: OEA) ha estado trabajando para fortalecer las capacidades de Seguridad cibernética entre sus Estados miembros desde principios de la década de 2000. Con los años se ha convertido en un líder regional en asistencia a los países para fortalecer la capacidad técnica y de Seguridad cibernética en cuanto a políticas para garantizar un ciberespacio seguro y resiliente. El Programa de Seguridad Cibernética de la OEA apoya las iniciativas sobre la base de un análisis en profundidad y la comprensión de la magnitud de las amenazas (OEA, 2015).

En 2004, los Estados miembros de este organismo aprobaron la Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética, que abogaba por un esfuerzo coordinado de múltiples partes interesadas en la lucha contra las amenazas cibernéticas en el Hemisferio y proporcionaba un referente inicial para cultivar y guiar tal enfoque.

Los Estados miembros fueron extraordinariamente previsivos cuando adoptaron tal estrategia, ya que se ha mejorado la protección de la infraestructura de las TIC con el fortalecimiento de la capacidad de los gobiernos para responder y mitigar incidentes cibernéticos. Estos compromisos se han reafirmado y fortalecido con los años a partir de la adopción de numerosas

declaraciones oficiales, incluyendo la más reciente relacionada con el papel y las responsabilidades de la OEA y sus Estados miembros en la promoción de la Seguridad cibernética, la lucha contra la delincuencia informática y la protección de infraestructuras de información crítica (OAS, 2016).

Para el año 2007, la Unión Internacional de Telecomunicaciones (UIT) de las Naciones Unidas (ONU), publicó una Estrategia para la Cooperación y la Colaboración con y entre las partes, ello a partir del desarrollo unos pilares estratégicos así: "(…) i) Medidas legales; ii) Medidas técnicas y procedimentales; iii) Estructuras organizacionales; iv) Desarrollo de capacidades; y v) Cooperación internacional" (Agencia Especializada sobre Tecnologías de Información y Comunicación de las Naciones Unidas, ITU, 2014). Esto seguido de la Guía de Ciberseguridad Nacional de la UIT en 2011, y en 2014, la UIT lanza el Índice de Ciberseguridad Global (GCI, por sus siglas en inglés) con el objetivo de medir los programas de Ciberseguridad.

Para el año 2015, el Consejo de la Organización para la Cooperación y el Desarrollo Económico (OCDE), adoptó y publicó la Recomendación sobre Gestión del Riesgo de Seguridad Digital para la Prosperidad Económica y Social de la OCDE (OCDE, 2015). El principal aporte en la construcción colectiva es la incidencia sobre la adopción de enfoques desde la Gestión de Riesgos desde el cumplimiento de los principios de:

> [...] (i) sensibilización, adquisición de habilidades y empoderamiento; (ii) responsabilidad de los interesados; (iii) derechos humanos y valores fundamentales; (iv) cooperación; (v) evaluación del riesgo y ciclo de tratamiento; (vi) medidas de seguridad apropiadas y acordes con el riesgo y la actividad económica y social en juego; (vii) innovación; y (viii) planificación de la preparación y continuidad. (OCDE, 2015).

Para el año 2018, el Foro Económico Mundial (FEM, 2018, pp. 33-36) ha entregado el Cuaderno de Resiliencia Cibernética para la Colaboración Público-Privada (WEF, 2018), a partir del desarrollo de tres capacidades: solidez, resiliencia y Defensa. La solidez se define como "la capacidad de prevenir, repeler y contener amenazas". La resiliencia se define como "la capacidad de gestionar y solucionar violaciones exitosas". Y la Defensa se define como "la capacidad de adelantarse a, interrumpir y responder a ataques" (WEF, 2018).

Las escuelas de formación, los grupos de investigación y en general los técnicos se han involucrado y aportado a la construcción colectiva. Puede observarse cómo, el Instituto Potomac para Estudios de Políticas en 2015 expide el Índice de preparación cibernética y se fundamenta en la preparación de indicadores para determinar mejoras en las categorías: (1) Estrategia Nacional; (2) respuesta a incidentes; (3) delito informático y aplicación de la ley; (4) intercambio de información; (5) inversión en I+D; (6) diplomacia y comercio; y (7) defensa y respuesta a crisis[7] (Cyber Readiness Index 2.0).

El Modelo de Madurez de Capacidad de Seguridad Cibernética de Oxford (Oxford, 2016), muestra cinco dimensiones: "[…] Política y Estrategia de Seguridad Cibernética; (ii) cultura cibernética y sociedad; (iii) Seguridad cibernética, educación, capacitación y habilidades; (iv) marcos legales y regulatorios; y (v) estándares, organizaciones y tecnologías […]".

7 El Cyber Readiness Index 2.0 se basa en el anterior Cyber Readiness Index 1.0, marco metodológico para evaluar la preparación cibernética en cinco elementos esenciales: Estrategia Cibernética Nacional, respuesta a incidentes, delito electrónico y capacidad legal, intercambio de información e investigación y desarrollo cibernético. El Cyber Readiness Index 1.0 aplicó esta metodología a un conjunto inicial de treinta y cinco países. Para obtener más información sobre Cyber Readiness Index 1.0, véase: Melissa Hathaway, "Cyber Readiness Index 1.0," Hathaway Global Strategies LLC (2013), http:// belfercenter.ksg.harvard.edu/ les/ cyber-readiness-index-1point0.pdf.

El Manual es un instrumento para evaluar el nivel de comprensión de las diversas partes interesadas en la capacidad y madurez cibernética de un país.

También la Academia de Gobierno Electrónico en Estonia lanzó un Índice Nacional de Seguridad Cibernética en mayo de 2016, allí se establecen 12 áreas de evaluación de capacidades son:

> […] (1) Capacidad para desarrollar políticas nacionales de seguridad cibernética; (2) Capacidad para analizar las ciberamenazas a nivel nacional; (3) Capacidad para proporcionar educación sobre seguridad cibernética; (4) Capacidad para garantizar seguridad cibernética de base; (5) Capacidad para proporcionar un entorno seguro para servicios electrónicos; (6) Capacidad para entregar identificación y firma electrónicas; (7) Capacidad para proteger la infraestructuras críticas de la información; (8) Capacidad para detectar y responder incidentes cibernéticos 24/7; (9) Capacidad para gestionar una crisis cibernética a gran escala; (10) Capacidad para luchar contra los delitos cibernéticos; (11) Capacidad para llevar a cabo operaciones militares de defensa cibernética; y (12) Capacidad para proporcionar seguridad cibernética internacional. (National Cyber Security Index, 2016).

1.4. Elementos críticos de la política nacional de Seguridad Digital colombiana y su impacto para la investigación el desarrollo y la innovación.

A manera enunciativa me limito en señalar los elementos que se convierten en críticos y que impactan la investigación, el desarrollo y la innovación, así:

i. la elaboración y ejecución de los planes de fortalecimiento de las capacidades operativas, administrativas, humanas, científicas;

ii. la elaboración y ejecución del plan de fortalecimiento de las capacidades institucionales, operativas, administrativas, humanas, de infraestructura física y tecnológica del sector Inteligencia;

iii. el diseño de un modelo de Gestión de Riesgos de Seguridad Digital a nivel nacional;

iv. el ajuste al marco regulatorio del sector de Tecnologías de la Información y las Comunicaciones, teniendo en cuenta aspectos necesarios para la Gestión de Riesgos de Seguridad Digital;

v. la creación de una agenda estratégica nacional e internacional en temas de Seguridad Digital;

vi. la adaptación e implementación de un modelo de Gestión de Riesgos de Seguridad Digital a nivel nacional (MinTIC, 2015).

1.5. La investigación de la Ciberseguridad y la Ciberdefensa como elemento de la Política Nacional.

Son precisamente estas dimensiones las que centran el actuar de la presente investigación, específicamente la *dimensión estratégica 2* que señala la necesidad de "[…]Crear 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", de manera particular se establece que el "[…] el Ministerio de Tecnologías de la Información y las Comunicaciones creará y pondrá en marcha un tanque de pensamiento con las múltiples partes interesadas para abordar la Gestión de Riesgos de Seguridad Digital mediante la investigación, el desarrollo y la innovación". En este orden corresponde en virtud del rol de la academia establecer la identificación de las partes que participan y están vinculadas

con la investigación, el desarrollo y la innovación en temáticas asociadas a la Seguridad Digital, así como la identificación de las temáticas a ser investigadas y las metodologías para ello.

Es precisamente este lineamiento de actuación el que enmarca el presente documento, al establecer una aproximación al estado actual en el que se encuentra la Ciberseguridad y Ciberdefensa, en cada uno de los sectores que involucran a las diversas partes interesadas y con ello aportar a la construcción de la dimensión estratégica en referencia.

2. LAS DIVERSAS PARTES INTERESADAS DEL ECOSISTEMA DE SEGURIDAD DIGITAL COMO ACTORES PRINCIPALES DE LA INVESTIGACIÓN.

2.1. El entendimiento de una Estrategia de Ciberseguridad y Ciberdefensa Nacional por las diversas partes interesadas

El *Conpes de Seguridad Digital 3854 de 2016* ha entendido que las múltiples partes interesadas son en el Esquema Nacional de Seguridad Digital, el Gobierno nacional y los territoriales, las organizaciones públicas y privadas, la Fuerza Pública, los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil, quienes dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales, y quienes pueden ejercer distintos roles y tener distintas responsabilidades (Conpes 3854 de 2016). En ese contexto resulta fundamental entender los elementos que incorpora, para todos y cada una de las partes interesadas, una Estrategia de Ciberseguridad para su organización.

a. *Gobernanza.* La "buena gobernanza" según lo presenta (Cerrillo Martínez, 2007) se erige con base en los principios de participación, eficacia, coherencia, transparencia y rendición de

cuentas, (último término conocido como *accountability*); dichas directrices marcan la pauta para las diferentes políticas públicas caracterizadas por un trato más cooperativo y consensuado hacia la ciudadanía, según lo señalé en mi texto de doctorado. Bajo este concepto, es necesario el desarrollo, desde el nivel estratégico de las organizaciones, sean públicas o privadas, de un conjunto de principios, normas y valores, que enmarquen la política de Ciberseguridad. Allí se deberá establecer, además, quién es la autoridad que ejercerá el liderazgo, la estructura de la organización; las formas, procesos y procedimientos de coordinación al interior y al exterior de esta.

b. ***Desarrollo de capacidades Especiales***. La estrategia debe incorporar un conjunto de medidas tendientes a la creación, mantenimiento y fortalecimiento de cuatro grupos: uno de prevención de riesgos; en segundo lugar, otro de Gestión de Riesgos; en tercera instancia, un grupo especial de reacción defensiva frente a escenarios de confrontación; por último, un grupo de cibercriminalidad, cuyo objetivo esencial es la investigación de ataques a la Infraestructura Crítica del Estado.

c. Formación. La estrategia debe contar con un plan a corto, mediano y largo alcance que permita la formación, en los distintos niveles -básico, técnico, profesional, especializado y experto- del conjunto de servidores de la organización. De la misma manera, deben existir unos elementos mínimos de formación para los usuarios o ciudadanos que se relacionan con la organización. Dicho plan de capacitaciones debe tener como principios la integralidad, transversalidad, permanencia, la prospectiva y la responsabilidad.

d. Esquema para prevención del riesgo, gestión de incidentes y Defensa de la Infraestructura Crítica. En la estrategia será necesaria la incorporación de tres elementos específicos, señalándose en cada uno de ellos los procesos, procedimientos, responsables, responsabilidades, y esquemas

de reacción que tengan que ver con los elementos que a continuación se relacionan. En primera instancia, la prevención de los riesgos, esto es, todas las medidas humanas, técnicas, institucionales, personales, económicas y políticas, necesarias para la prevención de los riesgos; En segundo lugar, tenemos la gestión de incidentes; se deben establecer las técnicas, procesos y procedimientos que se tendrán que desarrollar frente a un escenario en el que se vea comprometida la infraestructura física y lógica de la entidad; Por último, se encuentra el conjunto de normas, procesos y procedimientos en caso de verse comprometida la Infraestructura Crítica de la organización, es decir, la capacidad de reacción y sus límites en un escenario de confrontación. Así las cosas, existe un elemento transversal que es señalar que la infraestructura física y lógica de la entidad es el corazón y cuáles son las capas en que se permite su intrusión y los niveles correspondientes.

e. Marco legal. Siendo este uno de los elementos esenciales de la estrategia, en el desarrollo de esta se debe identificar los elementos estructurales de regulación como pueden ser, identificación electrónica, servicios misionales, Gestión de Riesgos, gestión de incidentes, obligaciones, condición de Infraestructura Crítica, entre otros.

f. Marcos de cooperación y diplomacia. La estrategia debe contener los elementos esenciales de cooperación, relación y trabajo, en conjunto con situaciones de prevención y gestión de los riesgos; pero al mismo tiempo tiene que incluir el esquema de cooperación nacional e internacional frente a escenarios de conflicto.

g. Investigación, desarrollo e innovación. Uno de los elementos más importantes que deberá abordar la Estrategia de Ciberseguridad y Ciberdefensa en una organización, es la creación de un centro de investigación, desarrollo e innovación que se encuentre alineado con la política de I+D+i Nacional y la genera-

ción de investigación desde la participación activa de las diversas partes interesadas. Partes que están definidas seguidamente.

2.2. Las diversas partes interesas en la Gestión de Riesgos de Seguridad Digital

2.2.1. Consideraciones preliminares.

El concepto de grupo de interés o partes interesadas[8] proviene de la consolidación de la Responsabilidad Social Empresarial (en adelante: RSE) o Responsabilidad Social Corporativa (en adelante: RSC) como área de estudio y aplicación por parte de las entidades del sector productivo. En este contexto se busca la identificación de aquellas colectividades u organizaciones a quienes influencia la actividad de una corporación o empresa, ya sea de manera directa o indirecta, y como tal, según Strandberg (2010), tienen derecho a ser escuchadas más no a que la empresa u organización satisfaga todos sus requerimientos.

En el campo de la RSE, por ejemplo, pueden identificarse grupos de interés observando el desarrollo de la línea de negocios como tal, esto es, desde las actividades que generan productores, proveedores, distribuidores o consumidores, si se toma al sector de transformación.

Otro modo, *a priori*, de detectar grupos de interés en este ámbito es a través de la determinación de Áreas de Influencia Directa (en adelante: AID) y Áreas de Influencia Indirecta (en adelante: AII) de una actividad industrial, extractiva o de infraestructura que, de cualquier forma, tienen impacto social y medio ambiental, para así encontrar a los interesados dentro de estas áreas.

8 "Se entiende por *stakeholder* cualquier individuo o grupo de interés que, de alguna manera — explícita o implícita; voluntaria o involuntaria— tenga alguna apuesta hecha — *to stake*, poner algo en juego— en la marcha de la organización […]" (OCDE, 2015).

Una similitud que se observa en cuanto a los grupos de interés en la RSE y en los que se dan en las relaciones de la producción académico científica, consiste en que lo que se genera en tales círculos ofrece resultados con finalidades específicas y con diferentes grados de impacto en diversas esferas de la sociedad; otra característica en común es la necesidad de buscar sinergia y realimentación entre la organización y sus grupos de interés, en concordancia con Strandberg (2010), quien señala que:

> […] El desarrollo de compromisos con los grupos de interés puede conllevar beneficios, pero si se establecen con grupos equivocados o se plantean de manera errónea pueden llevar a un desaprovechamiento de los recursos y distraer a la organización de otras prioridades más urgentes. Por ello, es importante considerar los objetivos estratégicos de la empresa (**o del proyecto, o del departamento en cuestión**) a la hora de plantearse por qué establecer una colaboración. […] (p. 11) [negrillas fuera del original]

Ahora bien, si se extrapola el tema 'grupo de interés' del terreno corporativo al de la investigación académica aplicada, los objetivos de esta deben confluir con los de los grupos de interés hacia los que van dirigidos los resultados de tal producción científica, lo cual tendría que redundar en beneficio no solo de determinadas empresas y sectores sino de la nación en su conjunto.

Igualmente, una de las principales diferencias en cuanto al compromiso con los grupos de interés en la RSE y aquellos que se puedan establecer desde producción científica, concebida en la academia, es el grado de compromiso en este último caso; por ende, en principio, sí se tendrían que cumplir los requerimientos de los grupos de interés que se beneficien con lo producido a partir de una línea de investigación como esta; pero ello solo debería darse sobre la base de acuerdos claros y medibles en cuanto a lo que se puede y debe brindar, de ahí

la importancia de determinar adecuadamente cuáles son los grupos de interés.

2.2.2. Modelos para identificar grupos de interés en la RSE.

Según Strandberg (2010), la organización AccountAbility sugiere tener en cuenta las dimensiones para identificar partes interesadas o grupos de interés, de acuerdo con el grado en que se presenten las siguientes circunstancias con ciertos colectivos: "Responsabilidad […] Influencia […] Tensión […] Dependencia […] Perspectivas diversas (identificación de oportunidades)" (p. 11).

Entonces, aquellos con quien se llegue a dar estas circunstancias, identificadas como dimensiones, son quienes harán parte de los grupos de interés. Adicionalmente, el mencionado autor, refiere que la Global Reporting Initiative menciona que la **proximidad de los grupos** y la **representación de organizaciones** son otros factores para tener en cuenta al determinar a las partes interesadas; estos factores son patentes cuanto se habla de AID y AII, según se mencionó en acápites anteriores.

Por su parte, Granda Revilla y Trujillo (s.f.) además de mencionar varias de las dimensiones y factores aludidos por Strandberg, pero enmarcados como perspectivas, añaden que por temas de economía es necesario realizar un proceso de **priorización** (donde se agrupen grupos con intereses similares), y previamente a esto se debe hacer "un ejercicio de agrupación de los stakeholders [sic] de interés, que permita unificar aquellos que la organización considere asimilados (similares características o expectativas) y facilite la posterior priorización" (p. 3).

Estos autores afirman que dicha priorización permite "una reflexión en torno a qué grupos de interés debe considerar como prioritarios y por tanto establecer mecanismos de diálogo más

intensivos […] y qué grupos de interés deben quedar en un plano secundario" (p. 3).

2.2.3. Metodología para identificación de grupos de interés en la línea de investigación.

Metodología Cualitativa – Descriptiva. Bajo este enfoque, se elige una estrategia cualitativa que pone "énfasis en procesos que no están rigurosamente examinados o medidos en términos de cantidad, monto, intensidad o frecuencia" (Schettini & Cortazo, 2015). Esto sin perjuicio de que la información así obtenida sirva como sustento para buscar datos cualitativos y estudiarlos.

De acuerdo con lo anterior, se plantea un estudio analítico del entorno usando investigaciones previas y documentos oficiales, como fuentes -teniendo en cuenta los factores y dimensiones presentados en los modelos de la RSE- para llegar al desarrollo de los siguientes aspectos:

- **Consolidación de información base**

1. Banco de información: consolidación continua de un banco de información con realimentación o actualización, basado en el marco teórico propio de la Gestión del Riesgo en Seguridad Digital y en los hallazgos de la investigación.

2. Determinación preliminar: gracias a la implementación del punto 1), se podrán establecer unos conjuntos o subconjuntos a quienes, en primera instancia, les resulta de interés lo generado a través de la investigación de esta línea.

- **Determinación de los grupos de interés**

Una vez hallados los conjuntos que requieren de los resultados de la investigación, se procederá a profundizar en tales

conjuntos y, teniendo el grado de incidencia de factores como: responsabilidad, influencia, dependencia, perspectivas diversas (oportunidades) se procederá a responder:

1. ¿Quiénes necesitan el producto de la investigación?

2. ¿Por qué lo necesitan y en qué medida?

3. ¿Cuál es el perfil de los destinatarios?

Esto incluye identificación de la agenda o interés de cada grupo, interés misional (si se trata de una institución o personal del Estado), interés comercial o corporativo entre otros.

4. ¿Qué beneficios y riesgos hay al divulgar la información contenida en los resultados? (Debe elaborarse una matriz)

5. ¿Quiénes se impactarán positiva o negativamente con el uso que, los posibles grupos de interés les den a los resultados de la investigación? (Debe elaborarse una matriz)

6. ¿Cómo pueden colaborar los grupos de interés con los encargados de la investigación?

7. ¿Qué medidas de seguridad se deben tomar?

8. ¿Cuál es el impacto legal del manejo y distribución de los hallazgos de la investigación?

Preparado en el marco del desarrollo de la metodología.

Figura 9. Determinación de los grupos de interés

Productos de la investigación

Así, teniendo en cuenta el personal, los insumos establecidos se debe determinar:

1. ¿Qué tipo de entregables se generarán?

2. ¿El número de entregables requeridos por los grupos de interés concuerda con los que se deben producir?

3. ¿El número de entregables requeridos por los grupos de interés concuerda con lo que necesitan verdaderamente?

4. ¿Quiénes serán los interlocutores entre los grupos de interés y la línea de investigación?

Preparado en el marco del desarrollo de la metodología

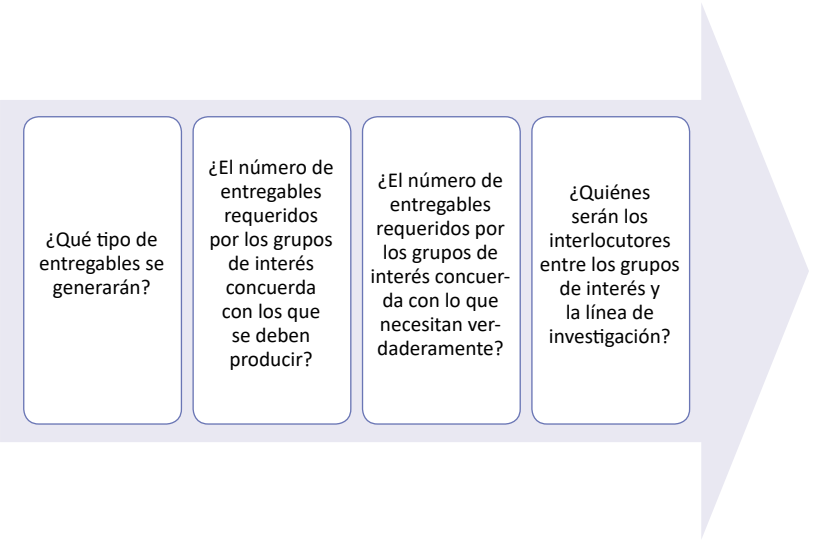


Figura 10. Productos de la investigación

En este orden se ha identificado que los grupos de interés corresponden a los sectores que hacen parte del ecosistema digital, a saber: i) el sector Gobierno; ii) el sector Defensa; iii) el sector Universitario y Académico; iv) el sector mixto y privado. Todos estos sectores que debe establecerse un contexto inicial en cuanto a la Gestión de Riesgos de Seguridad Digital que fundamente las temáticas de investigación en la línea correspondiente. Todo ello soportado sobre el concepto de Infraestructura Crítica Cibernética Nacional en los términos del documento *Conpes de Seguridad Digital para Colombia:*

> […] entendida esta como aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servi-

cios esenciales para los ciudadanos y para el Estado y cuya afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública (Conpes, 2016).

CAPITULO II

LA SEGURIDAD DIGITAL EN EL ENTORNO DE LA FUERZA PÚBLICA DIAGNÓSTICOS Y AMENAZAS DESDE LA GESTIÓN DEL RIESGO[9]

Jairo Becerra[10]
Ivonne León[11]
Escuela Superior de Guerra

Introducción

La aparición de nuevas tecnologías de la información y la comunicación introdujo en el escenario internacional la posibilidad de *virtualizar* la guerra y con ella, una serie de transformaciones en la estructura del Estado cuyo propósito fundamental es reaccionar ante nuevas amenazas. La revolución tecnológica ha enfrentado al planeta entero con la posibilidad de un ciberataque en diversos niveles que podrían comprometer lo militar, político, económico y social.

9 Capítulo de libro resultado del proyecto de investigación titulado "Gestión de Riesgos en Seguridad Digital" de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra, que a su vez hace parte de la línea de investigación 'Seguridad digital' del grupo de investigación 'Masa Crítica', reconocido y categorizado en (C) por Colciencias. Registrado con el código COL0123247, está adscrito a la Escuela Superior de Guerra de la República de Colombia.

10 Abogado, Investigador asociado de Colciencias E, Investigador en Derecho público y TIC, con más de 15 publicaciones en el campo de las TIC y ponencias nacionales e internacionales. Docente, Investigador de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto". Patrocinado por el Ministerio de Tecnologías de la información y las comunicaciones.

11 Magíster en Derecho y Politóloga (Universidad Nacional de Colombia). Experiencia en investigación, destrezas en la elaboración de trabajos escritos de carácter científico y técnico. Investigadora de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto".

La cuarta revolución tecnológica amplió el espectro de amenazas a las cuales deben responder los Estados. Un ejemplo de ello lo representan los ataques terroristas cuya intensidad se magnifica por la percepción de inseguridad que se genera en la opinión pública. De esta manera, el ciberterrorismo se ha convertido en un arma de alcance mundial que amenaza al Estado, emporios empresariales e individuos indiscriminadamente.

Este fenómeno, ha planteado la necesidad de contar con medios seguros para la transmisión de datos (redes seguras). No obstante, la posibilidad de responder efectivamente ante las amenazas que vienen dadas por la guerra virtual se encuentra con la imposibilidad de delimitar fronteras claras para combatirlas, y con ello, la conciencia de que se trata de una problemática de carácter global ante la cual no es posible la cobertura total de los riesgos.

Estas preocupaciones son recogidas por la Asamblea General de la Organización de las Naciones Unidas en 1999, cuando plantea la posibilidad de que las nuevas Tecnologías de Información y Comunicación se utilicen con fines en contra de la estabilidad y la Seguridad internacionales. Para el año 2004, la Comunidad Andina plantea entre sus objetivos, prevenir, combatir y erradicar las nuevas amenazas a la Seguridad. Mientras la Organización de Estados Americanos crea una red hemisférica para la respuesta a incidentes de Seguridad de computadores.

A dos años de que se cumpla la segunda década del siglo XXI las hipótesis sobre la batalla por la primacía digital se extienden rápidamente. En el escenario internacional Estados Unidos y China ocupan las principales noticias en revistas como *The Economist* en su carrera por la fabricación de Tecnologías de Información y Comunicación que podrían impactar de manera decisiva en redes y sistemas armamentísticos de avanzada.

En Colombia, la cuarta revolución industrial y la aparición de nuevas tecnologías comporta un nuevo espectro de retos de

cara a la modernización del país. Los procesos de producción industrial cada vez más automatizados y los sistemas de inteligencia artificial, conllevan un alto grado de independencia en la toma de decisiones que termina por afectar ejes tan importantes para el Estado, como son la Seguridad y la Defensa de una parte, y nuevas demandas sociales derivadas de presiones laborales.

Para avanzar de cara a la revolución tecnológica, Colombia tendrá que enfrentar los aspectos relacionados con la política y la administración del Estado, el ambiente y la conectividad misma que implican las nuevas tecnologías. De esta forma, será necesario trabajar en torno a la gobernanza digital que implica aspectos como el gobierno electrónico, la participación a través de nuevas redes de información y la transparencia política. Así miso, es necesario considerar la infraestructura inteligente relacionada con las redes de interconexión y posibilidades para generar una ciudad inteligente y la transversalidad en las TIC (Portafolio, 2017).

En este orden de ideas, este documento presentará una conceptualización general a partir de la cual se pretenden evidenciar las problemáticas, amenazas y riesgos que enfrenta la sociedad contemporánea en el marco de la cuarta revolución tecnológica. En el segundo apartado, se profundizará en los riesgos tecnológicos y los avances logrados en este campo. Finalmente, en el tercer acápite se presentan las estrategias en perspectiva de futuro frente a la Gestión del Riesgo y la Seguridad Digital.

1. NUEVAS TECNOLOGÍAS, UN NUEVO MUNDO

Las Tecnologías de Información y Comunicación han representado una nueva dimensión de posibilidades y amenazas en el mundo contemporáneo. Los sectores público y privado han incorporado dentro de sus procesos el uso de herramientas tecnológicas que disminuyen costos y hacen posible ofrecer respuestas ágiles frente a problemas cotidianos. La cuarta revo-

lución industrial ha significado de esta forma, una trasformación profunda en las actividades cotidianas y una disminución significativa en el tiempo requerido para actuar, generando también un marco para la transparencia y el acceso oportuno a la información.

En este apartado se presentan las características de la revolución de la información y la comunicación, evidenciando sus alcances y las principales transformaciones que esta produjo en el marco de la globalización. En el segundo apartado se presentan las nuevas tecnologías haciendo énfasis en la aparición de los sistemas ciberfísicos y el Internet de las cosas. Finalmente, el tercer punto volverá sobre los actores en el contexto de la cuarta revolución tecnológica y la globalización que comparten el nuevo escenario internacional con el Estado.

1.1. La Revolución de la Información

Las últimas décadas del siglo XX y las primeras del siglo XXI estuvieron marcadas por la globalización y la intensificación de la interconexión de redes económicas, políticas, culturales y militares. La cuarta revolución tecnológica profundizó las consecuencias de la globalización a partir de los avances en computación, tecnología digital, robótica, inteligencia artificial, impresión 3D, nanotecnología y computación cuántica, entre otras.

El concepto de Revolución 4.0 fue presentado por primera vez como una directriz del gobierno alemán en la Feria de Hannover realizada en 2011. Allí se planteó la necesidad de una Estrategia de Alta Tecnología como parte del programa marco *Horizonte 2020*. Las características de la propuesta recogían la estandarización, la posibilidad de que los dispositivos se configuren automáticamente (*plug and play*) y una producción interconectada digitalmente.

El eje principal de la Tecnología 4.0 es la información y su integración en procesos en los que no es posible distinguir entre elementos, ámbitos y niveles de producción. Estas nuevas tecnologías actúan como una extensa Red Neuronal de procesadores sociales de información y de conocimiento cuya lógica de interconexión es altamente compleja. La industria que surge a partir de estas nuevas tecnologías requiere para su funcionamiento de estructuras altamente flexibles que pueden ser rápidamente modificadas o reordenadas (Minsky, 1988, pp. 17-19; Castells, 2006, pp. 87-90).

Los cuatro rasgos predominantes de estas redes son instantaneidad o comunicación en tiempo real, interactividad o comunicación bidireccional, virtualidad o amplitud comunicacional, y unicidad o integración comunicacional. Todo esto se encuentra asociado a la posibilidad de generar nuevos mecanismos de organización tanto en el ámbito político como en el económico y nuevas formas de relacionamiento que no dependen de una infraestructura física ni de una territorialidad determinada.

> Así, la instantaneidad soporta la globalidad, en el sentido de que, en ausencia de distancia física y técnica, la comunicación se puede establecer, indiferentemente, con cualquier punto de la aldea global. Nuevas organizaciones de escala planetaria. Nuevas formas y fórmulas organizativas en el ámbito local y en el global. Por su parte, la interactividad contribuirá a la desmasificación de los medios. Frente a la unidireccionalidad de los medios de comunicación de masas, la bidireccionalidad de la red telefónica y telemática configura a todo elemento de la red como emisor/receptor de señales, no sólo receptor pasivo. La comunicación punto a punto fragmenta las audiencias masivas (Bericat Alastuey, 1996, p. 104).

La globalización y la aparición de nuevas Tecnologías de Información y Comunicación generaron nuevas formas políticas cristalizadas en nuevas herramientas de gestión, la recomposición de la administración pública hacia modelos de gobernanza horizontal y cooperativa, y una ciudadanía orientada por la inclusión, la equidad y la participación eficaz. Todo esto lleva a la necesidad de plantear un Estado con las capacidades necesarias para concertar, coordinar y dirigir a la sociedad hacia sus metas de desarrollo (Rivera Méndez, 2010, p. 3).

La gobernanza transforma no solo las estructuras organizacionales e institucionales, sino que afecta las prácticas sociales y los métodos de creación, acceso y divulgación del conocimiento. De esta manera, se puede definir la gobernanza como la organización de la acción o toma de decisiones colectivas, que incluye mecanismos formales e informales para el uso de las reglas, todo ello coordinado por actores estatales y no estatales (Neiva Santos, pp. 49-53, citado por Reyes Beltrán, 2017, p. 59).

De esta manera, la cuarta revolución industrial comporta la aparición de nueve tecnologías cuyas transformaciones han tenido impacto en los sistemas de producción e información a escala global. Estas tecnologías son Internet de las cosas, sistemas ciberfísicos, realidad aumentada, simulación, robótica colaborativa, fabricación aditiva, *big data*, *cloud computing* y Ciberseguridad.

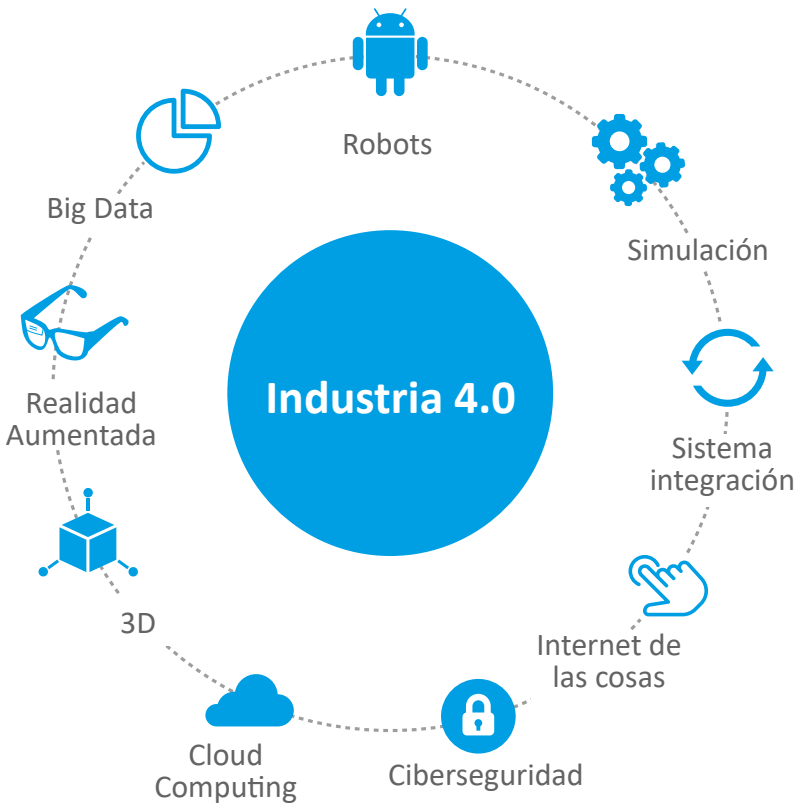


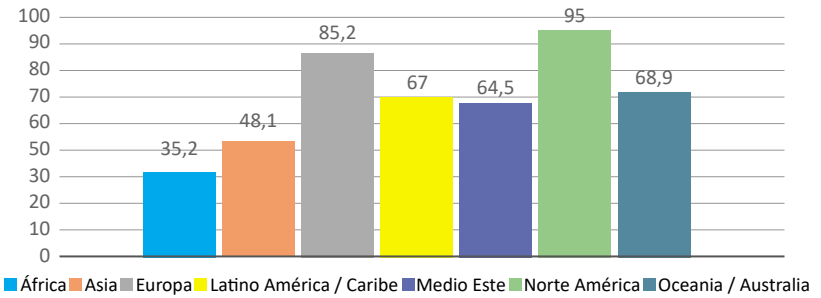
Ilustración 1. Industria 4.0.
Fuente: Paredes (2017) a partir de AMETIC

La integración horizontal y vertical de los sistemas permite la automatización de los procesos a través de la articulación de la información y comunicación entre diversas unidades y funciones. El Internet de las cosas hace posible la innovación de materiales y herramientas que coadyuvan en la elaboración de análisis descentralizados, mientras la nube facilita el almacenamiento y la disposición de información más allá de límites espaciales o territoriales con el propósito de disminuir el tiempo de reacción, consiguiendo la toma de decisiones con mayor agilidad. De otra parte, la simulación, los robots autónomos, la realidad virtual y la fabricación adaptativa permiten generar

innovaciones en menos tiempo y con mayor calidad, transitando hacia dispositivos que emplean información orientada hacia sistemas de preferencias y automatización.

1.2. Nuevas Tecnologías

Internet es un sistema mundial de información que funciona de manera descentralizada. Esta red se ha convertido en la autopista de información pública y de interconexión de ordenadores más extendida del planeta. De acuerdo con las cifras presentadas por la agencia de *marketing* y comunicación *We are Social*, la Web internacional *Internet World Stats* y *World Telecommunication Indicators Database* de la Agencia Especializada sobre Tecnologías de Información y Comunicación de las Naciones Unidas (ITU), a diciembre de 2017 aproximadamente el 50 % de la población mundial cuenta con acceso a Internet con un total aproximado de 4160 millones de habitantes.

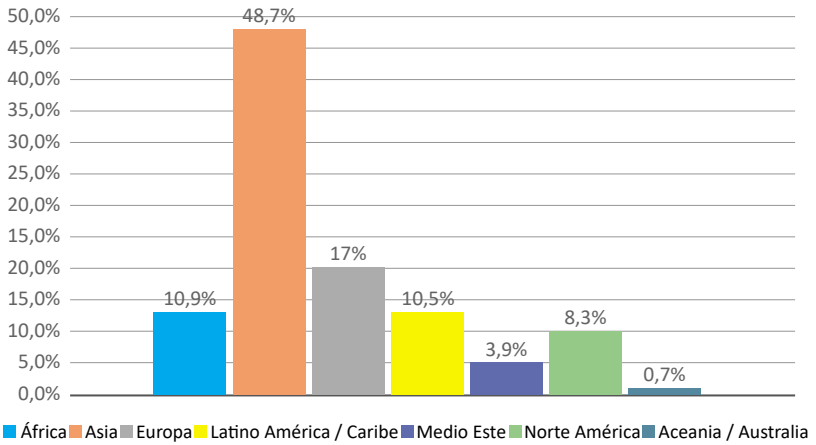


Gráfica 1. Tasa de Penetración de Internet (% Población

Fuente: Internet World Stats, 31 de diciembre de 2017

El mayor grado de penetración de Internet se encuentra en Norteamérica con 90 % aproximadamente, seguido por Europa con un 85 %, América Latina y el Caribe por su parte, cuentan con una penetración del 67 % seguido de cerca por Oriente Medio con un porcentaje de penetración del 64 % aproximadamente. Estos datos contrastan con el nivel de usuarios que se ubican

en mayor proporción en Asia con un 48 %. No obstante, vale la pena señalar que las estadísticas acerca del acceso a Internet, su porcentaje de penetración y el número de usuarios por región, varían rápidamente y parecen mantener una tendencia de aumento sostenido entre 2000 y 2018.



Gráfica 2. Usuarios de Internet.

Internet World Stats, 31 de diciembre de 2017

El Internet ha llevado a la comunicación e interacción digital en tiempo real entre diferentes objetos mediante Internet a través de redes fijas e inalámbricas, en lo que se conoce como el Internet de las Cosas o en inglés Internet of Things, IoT. Esta tecnología ha sido empleada en objetivos diversos como relojes, alarmas, sensores de velocidad, entre otros y ha implicado considerar que cualquier objeto puede ser un potencial generador de datos o de información.

Para que esta tecnología llegara a ser de uso cotidiano fue necesario la miniaturización de componentes, llevando a la generación de elementos cada vez más pequeños (*chips* y circuitos), lo que hace que se pueda conectar prácticamente a cualquier cosa, desde cualquier sitio, en cualquier momento. Así mismo,

se requirió la superación de la limitación de la infraestructura de telefonía móvil, y la proliferación de las aplicaciones y los servicios que ponen en uso la gran cantidad de información creada a partir del IoT (Fundación Bankinter, 2011, p. 6).

Los objetos interconectados a través Internet posibilitan la generación de entornos inteligentes capaces de analizar, diagnosticar y ejecutar funciones, disminuyendo la ocurrencia de errores humanos. La interconexión entre los objetos se produce a partir de operaciones remotas, usando una dirección IP (Internet Protocol) para contactar con un servidor externo y enviar los datos recogidos, y de la misma forma, ser accedido para recibir instrucciones. Así, entre los objetos que hacen parte del IoT se puede distinguir entre aquellos que funcionan como sensores, los que realizan acciones y aquellos que combinan ambas funciones (Torres, 2014).

Ámbito	Dispositivos
Vestibles	Relojes, lentes, anillos, ropa, cinturones, etc.
Domestica	Alarmas, cerraduras, cámaras, refrigeradores, televisores, control de temperatura, riego de jardines, etc.
Industriales	Variedad de sensores para monitorear y controlar producción, monitorear estado físico y ubicación de los empleados, etc.
Ciudades inteligentes	Detectores de velocidad, sensores para monitorear el tráfico, sensores en las estructuras de los edificios para monitorear su estado, cámaras de vigilancia, estacionamientos inteligentes, vigilancia mediante drones, etc.

Tabla 1. Clasificación de Dispositivos IoT
Tomada de Martínez, Mejía, Muñoz y García (2017, p. 81)

El Internet de las Cosas tiene como principio funcional las tecnologías máquina a máquina (M2M), que permiten la comunicación entre aparatos, captando información y convirtiéndola en acciones puntuales. En este esquema, M2M utiliza un dispositivo (como un sensor o medidor) para capturar un evento

(como la temperatura, nivel de inventario, etc.), que se retransmite a través de una red hacia una aplicación (*software*), que traduce a su vez el evento capturado en información significativa (Molano, 2014).

Internet de las Cosas, agrega una nueva dimensión a la comunicación al permitir la comunicación en cualquier momento y lugar dando lugar a la posibilidad de generar respuestas autónomas, para lo cual es fundamental el involucramiento de la inteligencia artificial (García, 2015, p. 17). Es así como este sistema crea una extensa red que se asimila a una compleja red neuronal, con capacidad de proveer datos y analizarlos en tiempos récord y eficientemente, para lo cual se apoya a su vez, en tecnologías como el *Big Data* y la inteligencia artificial.

La integración en la comunicación posibilitada por el IoT llevo a la generación de Sistemas Ciber-físicos o Cyber Physical Systems (CPS), que consiste en dotar a los objetos de capacidades computacionales y de comunicación con el propósito de convertirlos en objetos inteligentes que pueden cooperar entre ellos, formando ecosistemas distribuidos y autónomos (Fernández y Sáez Domingo, 2015, p. 5). Estos sistemas comportan un alto grado de adaptación y autonomía, y su aplicación se extiende a múltiples posibilidades que abarcan desde la movilidad y la salud, hasta extensos complejos sociales como la interconexión en ciudades inteligentes.

La cibernética y la inteligencia artificial aportan elementos para generar el acople entre diversos niveles tanto de orden horizontal como vertical con el propósito de consolidar sistemas flexibles con una capacidad de respuesta eficiente y ágil frente a problemas complejos. La cibernética mantiene el sistema en funcionamiento, permitiendo reajustes a los caminos iniciales o a nuevos caminos donde ha habido desvíos u obstáculos, para adaptar el mecanismo a los objetivos establecidos (Bericat Alastuey, 1996, p. 107; Bell, 1984, pp. 47-48).

De esta forma y teniendo en cuenta los conceptos desarrollados a partir de la cuarta revolución tecnológica, se puede entender que el Estado reoriente su estructura hacia instituciones flexibles que buscan la resolución eficiente de conflictos y problemáticas sociales, políticas y económicas, con el propósito de avanzar en torno a objetivos concretos. En este esquema de funcionamiento, la retroalimentación es fundamental toda vez que permite generar los mecanismos de reajuste del sistema. El Estado como la sociedad es policéntrico, mientras la información se presenta en mecanismos descentralizados.

1.3. Nuevos Actores

Con las nuevas Tecnologías de la Información y la Comunicación -TIC, emergieron nuevos actores políticos en los ámbitos locales e internacionales. Las redes de información favorecen las transacciones económicas, las trasferencias electrónicas de servicios especializados y la comunicación de grupos en diferentes lugares del planeta. Como anota Saskia Sassen,

> Las nuevas TIC, en especial la Internet de acceso público, han reforzado esta política de lugares y han expandido el espacio de los actores de la sociedad civil más allá de la red de ciudades globales, para abarcar también en algunos casos las localidades periféricas (Sassen, 2015, p. 236).

En este contexto, el Estado desaparece o tiende a la fragmentación en un proceso que presiona su reconfiguración y su adaptación a una nueva realidad. Se produce una reformulación de las escalas en términos de los lugares estratégicos que articulan el nuevo sistema, generando a su vez, las condiciones necesarias para que asciendan las ciudades, regiones y zonas transfronterizas (escala subnacional), así como mercados electrónicos globales y otras entidades supranacionales (Reyes Beltrán, 2017, p. 62; Sassen, 2015, p. 43).

En este contexto, el Estado se ve limitado por nuevas instituciones y entidades cuyo carácter dinámico no logra ser regulado por marcos jurídicos nacionales. Esta situación requiere un abordaje sistémico en el que diferentes actores asuman la responsabilidad frente a los riesgos que representa un contexto cada vez más interconectado. Así mismo, los marcos jurídicos se transforman rápidamente conforme a las reglas del Derecho Internacional, con decisiones que pueden influir en el sistema financiero global.

Todo esto, hace necesario construir y consolidar nuevos conjuntos de datos para rastrear los movimientos de información, capital y personas (Sassen, 2015, pp. 44-45). La desterritorialización del riesgo ha supuesto la necesidad de avanzar en los estudios y análisis de las interacciones entre naturaleza, tecnología y sociedad en contextos geográficos y espaciales a distintas escalas y niveles. El acople de las instituciones como un sistema global se presenta desde esta perspectiva como una respuesta al contexto de las sociedades complejas y globalizadas para dar cuenta de la diferenciación funcional (Reyes Beltrán, 2017, p. 153; Luhmann, 2007, pp. 3-10).

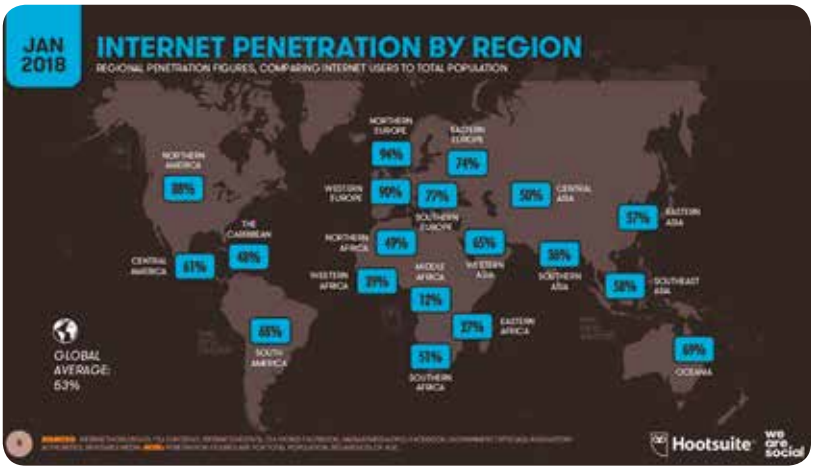
El nuevo contexto refuerza la actividad de organizaciones multilaterales de alcance regional y de naturaleza global. En la misma medida se ha reforzado el papel de actores no estatales como las Empresas y Organizaciones No Gubernamentales. Esta descentralización de las relaciones internacionales se da en el marco de las interacciones globales como en el ámbito del diseño de políticas nacionales de los Estados.

En este marco, es indispensable el establecimiento de una agenda internacional los Estados y los actores subnacionales para posibilitar una acción externa coordinada que refleje los diversos intereses de las naciones. La diplomacia adquiere un carácter descentralizado y supranacional, en el que se tienen en cuenta la multiplicidad de actores que interactúan en la comple-

ja red de vínculos internacionales (Orozco, 2016, pp. 193-196).

Un reflejo de este escenario internacional tuvo lugar en 2011 con la celebración del primer foro denominado *e-G8* en el que participaron los presidentes y primeros ministros de Estados Unidos, Alemania, Francia, Gran Bretaña, Canadá, Japón, Italia y Rusia, junto a 22 directivos y personalidades del sector de Internet. En este foro se discutió la visión común sobre Internet y el modelo económico a aplicar para garantizar su desarrollo.

> Internet supone el 3.4 % del Producto Interno Bruto (PIB) en 13 países, entre los cuales figuran los del G8 y tres las principales economías emergentes, China, Brasil e India. Además en los últimos cinco años Internet contribuyó en 10 % de su crecimiento, según un estudio dado a conocer en el e-G8 de París donde los fundadores de las principales redes sociales y del mayor buscador de Internet, abogaron "por un acceso libre y abierto" a Internet de todos los habitantes del planeta (Portafolio, 2011).



Mapa 1. Usuarios de Internet y Redes Sociales en el Mundo, 2018. Tomado de González (2018)

En una escala diferente, la interconexión entre los individuos de forma continua y permanente ha permitido que los movimientos sociales adquieran un nuevo sentido y orientación. Lo anterior, es potenciado gracias a la facilidad de convocatoria, el anonimato y el alcance de la difusión (Mariscal, 2016, p. 27). Las nuevas tecnologías, particularmente las redes sociales, han traído consigo el desacoplamiento gradual de la continuidad y la simultaneidad, haciendo posible una organización sin contigüidad.

> Algunas de las características más importantes de estos medios sociales son la interacción continua entre los miembros, la existencia de convenciones formales e informales, la voluntad de las personas para interactuar, la dimensión global y la velocidad con la que las relaciones se desarrollan (Uribe Saavedra, Rialp Criado y Llonch Andreu, 2013, p. 207).

La nueva sociabilidad creada por Internet se configura a partir de la creación de un espacio público de interacción en el que se facilita la creación de nuevas identidades colectivas y las interacciones entre los miembros de los movimientos sociales y de ellos con los medios de comunicación masiva y la prensa, multiplicando las posibilidades y frecuencias de comunicación entre individuos dispersos territorialmente (Mosca y Porta, 2009, pp. 194-202).

Las nuevas tecnologías de información pueden activar y revitalizar los movimientos sociales ya que permiten la planificación y ejecución de acciones y protestas, incluso antes de que se puedan producir reacciones o medidas para pararlas o contrarrestarlas. *Twitter* es un ejemplo del impacto que se genera a partir de líderes de opinión y que tienen la capacidad de situar temáticas coyunturales en la agenda mediática. El ciberespacio ofreció a los movimientos sociales la posibilidad de acceder a recursos de información a bajo costo en un proceso de difusión

de doble vía en el que es posible comunicarse y recibir retroalimentación con otros usuarios (De La Rosa, 2014, pp. 35-48; De La Rosa, 2016, pp. 48-49).

Al respecto es necesario analizar el considerable aumento en el uso de *smartphones* y *tablets*, así como la información relacionada con el acceso a redes sociales. En este sentido se debe anotar que cerca de un millón de personas empezaron a utilizar las redes sociales por primera vez de forma diaria en el último año, lo que significa que hay cerca de 11 usuarios de redes sociales nuevos cada segundo (González, 2018). Es así como las medidas restrictivas o preventivas frente a las acciones de movimientos sociales o de ciberactivistas se produce tarde, cuando miles de personas los han leído en las pantallas de sus computadoras, teléfonos móviles o *tablets.*

Los ciberactivistas son compuestos en gran proporción por jóvenes interesados en participar en el cambio social y que hacen parte activa de procesos de empoderamiento digital. Esta participación se explica, adicionalmente, por su dominio de recursos y aplicaciones tecnológicas, la independencia de los medios de comunicación a través de Internet que hacen posible poner en circulación mensajes con estructuras novedosas y el acceso a dispositivos móviles con acceso a Internet que posibilitan la creación y envió de información actualizada mediante plataformas dinámicas (De La Rosa, 2014b, p. 122).

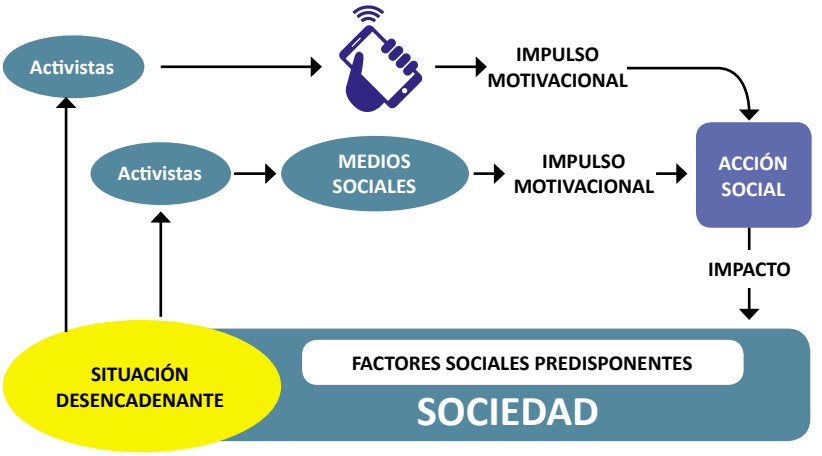


Ilustración 2. Los Movimientos Sociales en la Era Digital. Tomada de De La Rosa (2014b, p. 121)

Los *hacktivistas* representan un movimiento orientado por un tipo de acción política de resistencia y lucha por una sociedad alternativa, relacionada con la libertad de información, con las luchas por la democracia y por una sociedad abierta (Vicente, 2004, p. 3). Los *hacktivistas*, como los *hackers* y *crackers*, emplean conocimientos y técnicas en sistemas informáticos para adelantar movimientos de respuesta a políticas, normas o situaciones sociales que consideran regresivas o contrarias a sus motivaciones intelectuales o políticas.

Al respecto es importante contemplar las diferencias entre los diferentes actores que se involucran en el ciberespacio:

Hacker. Personaje apolítico, que solo lucha por sus compañeros, por la libertad de la información o por sí mismo.

Cracker. Su objetivo es crear virus e introducirse en otros sistemas para robar información y luego venderla al mejor postor.

Hacktivistas. Emplean sus habilidades en los sistemas infor-

máticos con fines políticos y sociales. Es decir, juegan al ataque y realizan lo que ellos llaman la Desobediencia Civil Electrónica (DCE) (Álvarez, 2013).

De otra parte, la aparición de poderes no institucionales favorecidos por las redes sociales y medios de comunicación de alcance masivo gracias a Internet, han representado un reto para las políticas públicas y la normatividad. La emergencia de nuevos actores en la escena internacional ha generado la emergencia de problemáticas asociadas a la corrupción y las economías ilegales, representando problemas de Seguridad pública que se suman a la sensación de inseguridad de la ciudadanía debido al aumento de los delitos y la actividad criminal (Maira, 2005, pp. 233-235; Reyes Beltrán, 2017, p. 144).

2. LA GESTIÓN DEL RIESGO Y LAS NUEVAS AMENAZAS GLOBALES

La aparición de las nuevas Tecnologías de Información y Comunicación ha transformado las sociedades contemporáneas. Internet posibilita el acceso a la información de manera asincrónica y sin límites en el tiempo y el espacio, conectando a las personas más allá de las barreras geográficas. El ciberespacio se ha convertido en el lugar de convergencia y negociación entre diversos actores que han replanteado los esquemas básicos de comunicación, situación que ha conllevado nuevos retos y amenazas en materia de regulación y políticas públicas.

En el nuevo escenario internacional las trasformaciones en la comunicación han conllevado igualmente, nuevos desafíos para la Seguridad y la forma de enfrentar las amenazas. En este apartado se explorará el estado actual de la cuestión, atendiendo a los riesgos del mundo contemporáneo. En el primer momento se hará reconstrucción de la Gestión del Riesgo desde sus abordajes teóricos y prácticos como respuesta a los nuevos desafíos de Seguridad. En

la segunda parte se presentarán las principales amenazas del ciberespacio a los Estados y los individuos. En el último apartado se establecerán los principales elementos que componen la visión de la Ciberdefensa desde las teorías de la Gestión del Riesgo.

2.1. La Gestión del Riesgo y los Desafíos de la Seguridad

El atentado al World Trade Center en New York, el 11 de septiembre de 2011, significó un cambio profundo en los marcos de sentido y de interpretación de asuntos como la Seguridad y la protección. Tal acontecimiento y sus consecuencias, situó a las sociedades globales frente a la posibilidad de que cada elección pueda tener consecuencias indeseadas o no calculadas con precisión. Como señala Josetxo Berian (2005), hoy la contingencia se presenta como un atributo moderno, que paradójicamente enfrenta el mayor conocimiento a través de la ciencia a un umbral de seguridades menor al de las sociedades tradicionales (p. 12).

La latencia de las amenazas y la necesidad de anticipar la catástrofe ha llevado a la posibilidad de restringir algunas libertades en favor de la consolidación de un marco de seguridad que se configura en torno a la sospecha más que de la realidad. Como lo explica Ulrich Beck (2008)

> […] el riesgo es el patrón perceptivo e intelectual que moviliza a una sociedad enfrentada a la construcción de un futuro abierto, lleno de inseguridades y obstáculos, una sociedad que ya no está determinada por la religión la tradición o la sumisión a la naturaleza y que tampoco cree en los efectos redentores de las utopías (p. 20).

La globalización y la revolución de la información ha generado que el riesgo adquiera características espaciales, temporales y sociales deslocalizadas, toda vez que un incidente puede generar efectos más allá de las fronteras del Estado como es el caso del cambio climático, perdurar en el tiempo como en el caso de un

ataque nuclear, o comportar un alto grado de complejidad social como en las crisis financieras (Casas Mínguez, 2016, p. 5).

La magnitud del riesgo está estrechamente ligada con la posición geoestratégica y el acceso a recursos como la información, lo que involucra, además, una competencia permanente por determinar las amenazas mundiales. Esta situación conlleva decisiones que en sí mismas comportan riesgos, toda vez que no existen opciones seguras o arriesgadas sino alternativas que dependen de su conmensurabilidad y que afectan ámbitos cualitativamente diferentes (Beck, 2008, p. 18).

Las amenazas se presentan en un espectro amplio y muchas veces indeterminable, que pasan por el terrorismo, el riesgo nuclear, la intervención genética y el calentamiento global, siendo estos fenómenos en los que se conjugan el saber y el no-saber en un espectro amplio de probabilidades. En este mismo marco, los Estados mismos se convierten en un riesgo inminente frente a otros Estados por efectos de problemáticas como la contaminación, la migración y la posibilidad de la guerra nuclear, entre otros.

Adicionalmente, los riesgos tienen un alto componente democratizador en virtud de un doble proceso de deslocalización. Por un lado, la amenaza puede comportar un alto grado de incertidumbre con respecto a su origen, por lo que es necesario avanzar con una concepción que vaya más allá del estatismo metodológico. De otra parte, en virtud de este mismo cosmopolitismo, las consecuencias del riesgo conllevan alcances inimaginados que se extienden rápidamente más allá de las fronteras nacionales.

El riesgo puede comprenderse en términos generales como la causa o probabilidad de un suceso no deseado que puede o no ocurrir. Desde el valor de expectativa, es posible comparar un factor de riesgo frente a otros en términos de un dato relevante, por ejemplo, el número de víctimas que puede causar. Y desde la teoría de la decisión se pueden tomar en consideración el conocimiento de

las probabilidades o la incertidumbre para diseñar cursos de acción (Hansson, 2000, citado en Lapuente Sastre, 2006 p. 5).

La percepción sobre el riesgo depende de complejos e imbricados sistemas culturales de creencias, valores e ideales que pueden ser modulados a través de las redes de información y comunicación (Tabernero, Moyano y Trujillo, 2014, p. 2). Así también, los criterios de evaluación del riesgo dependen en un alto grado de las diferentes clases de amenazas identificadas en contextos particulares de acuerdo con los intereses estratégicos de quien o quienes lo evalúan.

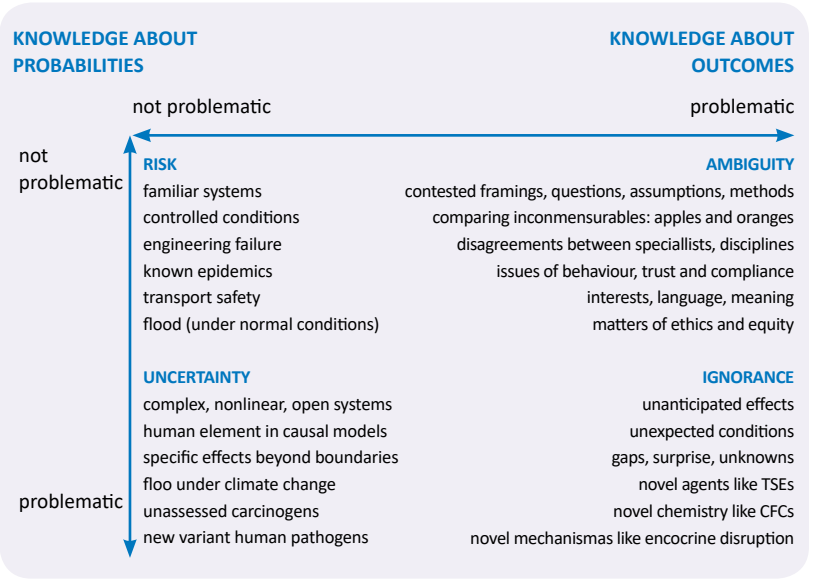
Las estrategias de gestión inteligente para el manejo de los riesgos dependen igualmente de estos intereses y de la posición respecto al espectro global del Estado que las pone en marcha. En este sentido es importante distinguir entre riesgo como amenaza potencial y riesgo como probabilidad de ocurrencia de un fenómeno no deseado. La claridad sobre los indicadores que permiten develar la probabilidad de que un fenómeno determinado ocurra, permite tomar decisiones graduales e inteligentes respecto al futuro (Tabernero, Moyano y Trujillo, 2014, p. 2).

Hay, en principio, cuatro estados de conocimiento lógicamente posibles pueden presentarse en la toma de decisiones, incertidumbre, riesgo, ambigüedad y desconocimiento (Stirling, 2009, pp. 330-331). La fiabilidad y calidad del conocimiento permite anticipar y responder al riesgo o a las amenazas de acuerdo con experiencias pasadas o efectos predecibles. De aquí se desprende el hecho de que hay riesgos que comportan un mayor grado de complejidad para su tratamiento. En un estadio de incertidumbre, por ejemplo, la probabilidad no existe por lo que los juicios adoptados comportarán a su vez, un alto grado de desconocimiento en cuanto a los alcances y resultados.

Cada uno de los estadios (riesgo, incertidumbre, desconocimiento, ambigüedad) son resultado de diferentes grados de

conocimiento sobre las probabilidades de ocurrencia de un fenómeno y sus resultados. En el plano real, los diferentes planos no son excluyentes entre sí, por lo que se pueden presentar en diferente intensidad. En un estadio de incertidumbre se pueden caracterizar los resultados posibles, aunque no se cuente con información sobre las probabilidades de ocurrencia, por lo que la forma de proceder es reconocer el carácter abierto de una variedad de posibles interpretaciones para dar respuesta a ellas.

En el ámbito de la ambigüedad se conocen las probabilidades, pero no es posible calcular o puede no haber acuerdo sobre los resultados. Este escenario refiere a acontecimientos que no pueden ser evitados o sobre los cuales se pueden encontrar referencias en el pasado. En el ámbito de ignorancia, no se pueden caracterizar ni las probabilidades ni los resultados, prima el desconocimiento sobre los acontecimientos y sus consecuencias (Stirling, 2009, pp. 327-333).



Gráfica 3. Estados posibles del conocimiento incompleto. Tomada de Stirling (2009, p. 329)

Así, teniendo en cuenta estas condiciones, Andreas Klinke y Ortwin Renn, "formularon su aproximación al análisis del riesgo basándose en nueve criterios de evaluación, seis clases de riesgos, un árbol de toma de decisiones y tres categorías genéricas para su gestión" (Tabernero, Moyano y Trujillo, 2014, p. 3). El nivel de incertidumbre frente a las probabilidades y el impacto de las consecuencias o de los resultados se traduce en este modelo en una escala de nivel de tolerancia del riesgo, que recoge el área normal, intermedia e intolerable.

Los nueve criterios de evaluación del riesgo (Klinke & Renn, 2001; Klinke & Renn, 2002) comprenden:

1. daño potencial
2. probabilidad de ocurrencia
3. incertidumbre
4. ubicuidad (dispersión y propagación geográfica de los daños potenciales)
5. persistencia (extensión temporal)
6. irreversibilidad
7. efectos de latencia (tiempo de retardo entre el evento y las repercusiones)
8. violación de la equidad
9. potencial de movilización

El objetivo de la Gestión del Riesgo es planear y disponer de estrategias viables y apropiadas para tomar decisiones. "Las estrategias de Gestión del Riesgo persiguen el objetivo

de garantizar la seguridad e integridad, transformando riesgos inaceptables en riesgos aceptables" (Tabernero, Moyano y Trujillo, 2014, p. 6). Las nuevas Tecnologías de Información y Comunicación obligan a estar preparados y ofrecer respuestas frente a riesgos de carácter global desde contextos complejos.

Con este propósito se proponen la Gestión de Riesgo basada en una perspectiva técnica, en el principio de precaución y en la deliberación. Desde el enfoque técnico, el riesgo se conceptualiza como una propiedad objetiva de los sucesos y actividades que involucran la tecnología. Esta perspectiva requiere un abordaje multidisciplinar que favorezca la convergencia conceptual para definir de forma apropiada los fenómenos y avanza en torno a herramientas de la estadística de variables en la búsqueda de una universalmente válida con ayuda de la cual puedan establecerse comparaciones entre distintas clases de riesgo (Rivera Berrío, 2009, p. 4; Tabernero, Moyano y Trujillo, 2014, p. 7).

La Gestión del Riesgo basada en el principio de precaución se asocia a un alto grado de incertidumbre, por lo que se requiere un método de evaluación de mayor complejidad. En este tipo de Gestión del Riesgo se involucran la mayor variedad de incertidumbres, posible, posibles escenarios, indicadores de posible daño, tendencias, partes interesadas y grupos sociales afectados para determinar la resistencia que se puede producir (Stirling, 2009, pp. 341-343). La precaución contempla la posibilidad de prohibir con fines preventivos y puede referir a fenómenos como los ataques cibernéticos o la biotecnología (Tabernero, Moyano y Trujillo, 2014, p. 7).

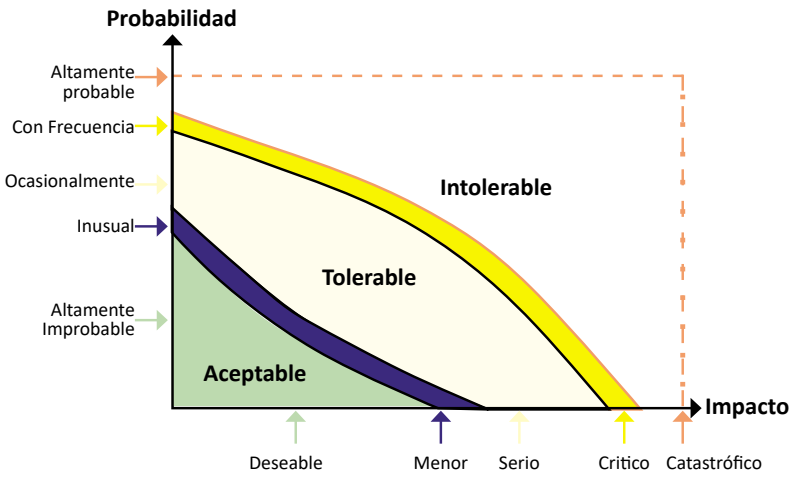
> Actuar con precaución es actuar con cautela para evitar posibles inconvenientes, dificultades o daños; es decir, cuando no hay suficientes razones para creer que un curso de acción está libre de riesgos. […] Un

> modelo racional es el denominado principio de precaución al que se acude cuando no se conocen los posibles impactos que genera la toma de decisiones de carácter técnico o científico; es decir, cuando los datos científicos o tecnológicos no permiten una evaluación del riesgo (Rivera Méndez, 2010, p. 5).

La gestión basada en la deliberación, por su parte, tiene en cuenta la discusión participativa acerca de las justificaciones, posibles beneficios, costes y riesgos de los factores involucrados con el propósito de resolver ambigüedades y diferencias. Este esquema de deliberación señala la necesidad de la participación democrática y la posibilidad de llegar a consensos en la búsqueda de soluciones compatibles con los intereses y necesidades de los afectados. Este esquema permitiría resolver o evitar los posibles conflictos derivados del riesgo.

Es así como a cada modelo de Gestión del Riesgo, le sigue un esquema de acción determinado ((Tabernero, Moyano y Trujillo, 2014, pp. 7-8). Con un esquema técnico, un alto nivel de daños y baja probabilidad de ocurrencia, las acciones estarán encaminadas a determinar la probabilidad, reducir el desastre potencial, incrementar la resistencia, prevenir y gestionar la emergencia. Una Gestión del Riesgo basada en el principio de precaución se puede poner en marcha en condiciones de incertidumbre frente a los daños y la probabilidad de ocurrencia, y las acciones estarán dirigidas a mejorar el conocimiento, reducir y contener la emergencia y evaluar la necesidad de aplicar prohibiciones.

Finalmente, la gestión basada en la deliberación puede incluir un rango de conocimiento sobre la probabilidad de ocurrencia y los posibles daños que abarcan tanto un alto como un bajo grado de incertidumbre. La participación puede ser empleada en este esquema con el propósito de Concienciar, transmitir confianza, comunicar el riesgo y gestionar las contingencias.



Gráfica 4. Estrategias de la Gestión del Riesgo. Tomada de Renn y Klinke (2012) por Moncada (2015).

En este contexto, las amenazas que enfrenta la Fuerza Pública deben tener un enfoque de Gestión del Riesgo que maximice la efectividad de las acciones emprendidas por esta, haciendo hincapié en que la magnitud del problema y sobre todo sus implicaciones, hacen necesario la prevención de actos que alteren el normal funcionamiento del entorno, cuyo incremento en diversidad y cobertura se enfoca de manera principal en la ciudadanía (Conpes 3854, 2016) y dificultan el accionar de las autoridades.

Es así como la Política Nacional de Seguridad Digital, establecida en el Conpes 3854, está enfocada en la Gestión del Riesgo y se basa en la atención de cinco problemas centrales:

Falta de visión estratégica en Seguridad Digital basada en la Gestión de Riesgos;

1. Las múltiples partes interesadas no maximizan sus oportunidades al desarrollar actividades socioeconómicas en el entorno digital;

2. El refuerzo de las capacidades de Ciberseguridad con un enfoque de Gestión de Riesgos de Seguridad Digital;

3. El refuerzo de las capacidades de Ciberdefensa con un enfoque de Gestión de Riesgos de Seguridad Digital; y

4. La necesidad de aumentar los esfuerzos y la articulación de cooperación, colaboración y asistencia, nacional e internacional, relacionados con la Seguridad Digital.

2.2. Ciberdefensa. Enfoques desde la Gestión del Riesgo

El orden inaugurado después de la crisis energética de 1970 involucró nuevos actores internacionales entre los cuales emergieron empresas de orden trasnacional y multinacional que transformaron el entorno geopolítico, económico y sociopolítico a nivel global. El modelo económico que supuso este nuevo orden conllevó un espacio altamente organizado y la aparición de relaciones que requieren un alto nivel de concertación en las escalas nacional, transnacional y supranacional.

Intervenciones sobre territorios geoestratégicos como Irak, Afganistán y Libia, reflejan la necesidad de consolidar y controlar espacios de acuerdo con un entorno global en constante trasformación. La complejidad del mundo contemporáneo debe apelar a una versatilidad de iniciativas y respuestas capaces de asegurar el acceso a fuentes de recursos estratégicos, la movilidad del capital y con ello, el establecimiento de una globalidad ordenada (Ceceña, 2008, p. 23).

> El impacto de la globalización en la regulación estatal es un fenómeno cualitativamente nuevo por dos razones: en primer lugar, reduce la intervención y regulación, ya que el movimiento actual produjo el debilitamiento de los poderes estatales, además de ejercer una presión sobre los Estados de forma monolítica bajo

> sus condiciones el modelo de desarrollo orientado hacia el mercado es el único compatible con el nuevo régimen global de acumulación. En segundo lugar, esta presión se refuerza con hechos tan dispares como el fin de Guerra Fría, las innovaciones tecnológicas de comunicación e información, los sistemas de producción flexible, la aparición de bloques regionales, la democracia liberal como régimen político universal y la imposición de la ley para proteger la propiedad intelectual (Santos, 2005, pp. 246-247).

En este contexto, los atentados del 11 de septiembre de 2001 al World Trade Center en Nueva York, marcó un punto de inflexión en los marcos interpretativos sobre la Seguridad y la protección, desplazándolos de referentes nacionales hacia un orden global cuya gestión se lleva a cabo bajo la óptica del riesgo (Beck, 2008, pp. 15-46). La posibilidad permanente de que eventos catastróficos tengan lugar, potencializada con el auge de las Tecnologías de Información y Comunicación, ha generado retos sociales, políticos, económicos y jurídicos cuya probabilidad de ocurrencia y consecuencias son difíciles de determinar.

Un primer problema de las nuevas Tecnologías de Información y Comunicación –TIC, está dado por la posibilidad de la comunicación de masas en una escala sin precedentes. Las nuevas formas de comunicación, cristalizadas en las redes sociales, se desarrollan a través de nuevas formas de interacción en las que la distinción entre lo público y lo privado se ve disminuida y eliminada; se relativizan el tiempo y el espacio favoreciendo interacciones de carácter predominantemente dialógicas cuya ubicación no se encuentra anclada a un espacio físico tangible; y es posible generar mensajes dirigidos a una masa de receptores sin que exista una orientación especifica de la acción (Muñoz, 2005, p. 560).

Las repercusiones políticas de este nuevo tipo de comunicación se han materializado en la posibilidad de convocar, gestio-

nar y ejecutar manifestaciones globales que adquieren móviles diversos que abarcan la demanda de derechos, el rechazo frente a fenómenos o decisiones que trascienden el ámbito nacional o la visibilización de intereses de sectores sociales diversos. Tal es el caso de las movilizaciones de rechazo a la intervención de Irak en 2003, el movimiento 15-M también conocido como movimiento de los indignados en 2011 y las manifestaciones del mundo árabe entre 2010 y 2013 conocidas como la primavera árabe.

Los riesgos tecnológicos se han clasificado según su voluntariedad (Starr, 1969), de acuerdo con su probabilidad de ocurrencia y el alcance o magnitud de sus consecuencias (Cohen & Lee, 1979); en función de la percepción que el público tiene de ellos (Fischhoff, Slovic, Lichtenstein, Read, & combs, 1978; Slovic, 1990). Sin embargo, uno de los más importantes aportes en este campo fue el producido por Hohenemser, Kates, & Slovic (1983), quienes clasificaron los riesgos tecnológicos de acuerdo con la extensión espacial de su impacto, el tiempo de duración entre exposición y consecuencias, la mortalidad humana anual, la mortalidad humana potencial, el impacto sobre generaciones futuras, entre otras categorías (Saurí, 1995, p. 151).

En coherencia con las teorías sobre la Gestión del Riesgo, los riesgos tecnológicos se pueden agrupar en tres grupos, a saber, riesgos extremos de carácter múltiple, riesgos extremos y riesgos ordinarios (Saurí, 1995, p. 151). La evaluación, por su parte, ha implicado nuevos restos para el ámbito jurídico-político, ya que aceptar un nuevo riesgo y determinar su carácter o alcance, implica generar nuevos desarrollos para hacerle frente y con ello, complejizar el sistema.

> Puesto que las decisiones tecnológicas, así como la identificación, estimación, valoración y Gestión del Riesgo no son asépticas ni están libres de intereses (económicos, políticos, ideológicos y religiosos), las

> conclusiones de una evaluación muy difícilmente serán unánimemente aceptadas (Rivera Méndez, 2010, p. 2; Olivé, 2004, p. 171).

La conceptualización y aceptación del riesgo se produce desde la construcción psicológica y tiene un carácter contingente. Esta creación del riesgo depende en buena medida de la creencia en que la acción humana puede prevenir el daño, por lo que es fundamental la posibilidad de construir escenarios futuros a partir de determinar los tipos de riesgos tecnológicos que se pueden producir y sus consecuencias determinadas.

Es así como, pese a que el Estado tiene la potestad de establecer y clasificar los riesgos a los cuales hacer frente, el sentido social del riesgo lleva a que cada individuo lo reconfigure de acuerdo con su propia experiencia. De esta forma, la conceptualización del riesgo tecnológico responde a un doble sentido, de abajo hacia arriba de acuerdo con la experiencia social y de arriba hacia debajo de acuerdo con las amenazas que el Estado considere prioritarias. Las percepciones y experiencia del individuo juegan, de esta forma, un papel importante en las creencias culturales, los principios y valores y los contextos económico, político y social en el que se crea y se recrea el riesgo (Renn, 2005, p. 23; OCDE, 2003, p. 67; Rivera Berrío, 2009, p. 2).

El ataque a las infraestructuras críticas de los Estados se encuentra entre una de las amenazas más importantes a nivel mundial. Al afectar los sistemas de suministros de servicios básicos tales como agua, luz y gas, se puede interrumpir seriamente el normal desarrollo de una sociedad y mermar su capacidad de respuesta colectiva. Así, avanzando frente a esta problemática, la *directiva 1148 de la Unión Europea* expedida en el 2016 ordena a todos los Estados miembros que identifiquen los operadores de servicios esenciales establecidos en su territorio para cada sector, entendiendo que de dicha acción se puede desprender la base para combatir amenazas potenciales

de desestabilización de un Estado, o en este caso de un conjunto de Estados.

La percepción de la sociedad frente al riesgo tecnológico puede estar determinada también, por el índice de penetración y la posibilidad de acceso a las TIC. De esta manera, los niveles de preparación de los Estados frente a las amenazas tecnológicas son muy distintos, lo que ha dado lugar a planteamientos fragmentados en temas como la evaluación y la percepción sobre sus consecuencias, lo cual influya a su vez, en niveles desiguales de protección de los consumidores y las empresas (Directiva UE 1148, 2016).

Los Estados comparten la responsabilidad frente a los riesgos tecnológicos con sectores públicos y privados, así como con individuos, en virtud de su rol diferenciado y su participación en las nuevas tecnologías de información.[12]

Un ejemplo de ello es la Active Cyber Defense Certainty Act (H.R. 4036, 2017) en los Estados Unidos. Consciente de los retos que conllevan las TIC, ha expresado que el ciberfraude y los crímenes relacionados con él, representan una amenaza grave para la Seguridad nacional y para la vitalidad económica de los Estados Unidos. Estos hechos presentan la necesidad imperiosa de la protección de la ciudadanía, en el ciberespacio, como un valor estratégico para el conjunto del Estado.

En este marco, la Defensa del territorio y la posibilidad de respuesta de los cuerpos de Seguridad del Estado son de vital im-

12 Al respecto la OCDE ha señalado lo que aquí se refiere: "All stakeholders should understand digital security risk and how to manage it. They should be aware that digital security risk can affect the achievement of their economic and social objectives and that their management of digital security risk can affect others. They should be empowered with the education and skills necessary to understand this risk to help manage it, and to evaluate the potential impact of their digital security risk management decisions on their activities and the overall digital environment" (OCDE, 2015, p. 9).

portancia. En el mundo globalizado contemporáneo, donde se requiere el acceso a grandes cantidades de información, las nuevas Tecnologías de Información y Comunicación son un elemento fundamental para el funcionamiento de la sociedad. "Esta necesidad de acceso e intercambio de información lleva inherentemente asociada la Seguridad, ya que dicha información debe estar protegida frente a accesos o modificaciones no autorizadas" (Escuela de Altos Estudios de la Defensa, 2014, p. 15).

Esta situación ha implicado que la localización de los riesgos sea cada vez más complicada, dando lugar a escalas geográficas globales en las que se dificulta establecer la localización de las amenazas o prever las infiltraciones a sistemas operativos, logísticos y de comunicaciones, lo que frecuentemente se suma a la falta de interés de las poblaciones afectadas y la ausencia de marcos regulatorios se convierten en límites para la innovación y retos para la Seguridad.

En las últimas décadas, los Estados han venido reorientando esfuerzos y recursos para resguardar no solo los espacios tradicionales (terrestre, marítimo y aeroespacial), sino también el ciberespacial (Cornaglia & Vercelli, 2017, pp. 46-62). La dimensión ciberespacial, sin locación física específica propia, genera replanteos sobre las tradicionales categorías con las que se aborda la guerra y exige, por la dinámica propia de la innovación tecnológica, una rápida adaptación para los Sistemas de Defensa respecto de sus componentes.

Una baja percepción del riesgo en materia tecnológica, de otra parte, podría asociarse a la idea de que el problema es difuso o está asociado a causas diversas difíciles de establecer, cuyas consecuencias solo se harán reales en el escenario de un futuro lejano. Esta falta de interés en los riesgos tecnológicos se explicaría, además, por la falta de familiarización de la sociedad con el uso de las nuevas Tecnologías de Información y Comunicación.

> De acuerdo con el paradigma psicométrico sobre la percepción del riesgo tecnológico, desarrollado por psicólogos y geógrafos a finales de los setenta, el público en general contrapone al criterio de mortalidad humana anual otros criterios para valorar el riesgo, como por ejemplo el grado de control individual sobre este, su impacto potencial sobre las generaciones actuales y futuras y la familiaridad con la tecnología en cuestión (Saurí, 1999, p. 152).

Uno de los elementos más importante en el ámbito de la Ciberdefensa es, entonces, asegurar el normal funcionamiento de la sociedad en el ciberespacio y entregarle la Seguridad necesaria en el desarrollo de sus actividades diarias. De esta forma, se intenta asegurar los niveles de confianza suficientes e indispensables para el desarrollo de actividades cotidianas asociadas en gran medida al empleo de tecnologías asociadas al Internet de las cosas, IoT, de forma tal que se genere el contexto necesario el desarrollo de todo el potencial de este espacio para la sociedad.

Son los particulares los que se enfrentan en su interacción diaria a la mayor cantidad de vulnerabilidades en el ciberespacio y así mismo, sus capacidades para actuar son limitadas. Por lo que se han hecho frecuentes las iniciativas que procuran informar e instruir a la ciudadanía frente a ataques de tipo *phishing* o ingeniería social; virus que acceden de forma no autorizada a los servidores de un servicio donde se almacenan las contraseñas de los usuarios o espías de las comunicaciones de red.

Frente a estas problemáticas, en Colombia la Policía Nacional ha puesto a disposición de la ciudadanía el Centro Cibernético Policial, con servicios como el análisis de *malware*, recomendaciones de Ciberseguridad, un centro de atención a denuncias virtual que constituye la primera iniciativa en Iberoamérica en atención en línea policial y aplicaciones móviles para el fortale-

cimiento de la Ciberseguridad, entre otros (Policía Nacional de Colombia; Ministerio de Defesa Nacional, 2018).

En este punto es relevante distinguir entre Ciberdefensa y Ciberseguridad. La Ciberseguridad o Seguridad cibernética se refiere al combate y prevención de crímenes cibernéticos en la esfera de la Seguridad pública o por parte de entidades del Estado. La Ciberdefensa o Defensa cibernética, responde a un conjunto de acciones defensivas, exploratorias y ofensivas orientadas por Fuerzas Militares en un ejercicio de planeación estratégica para la salvaguarda de la seguridad nacional (López, 2013, p. 27).

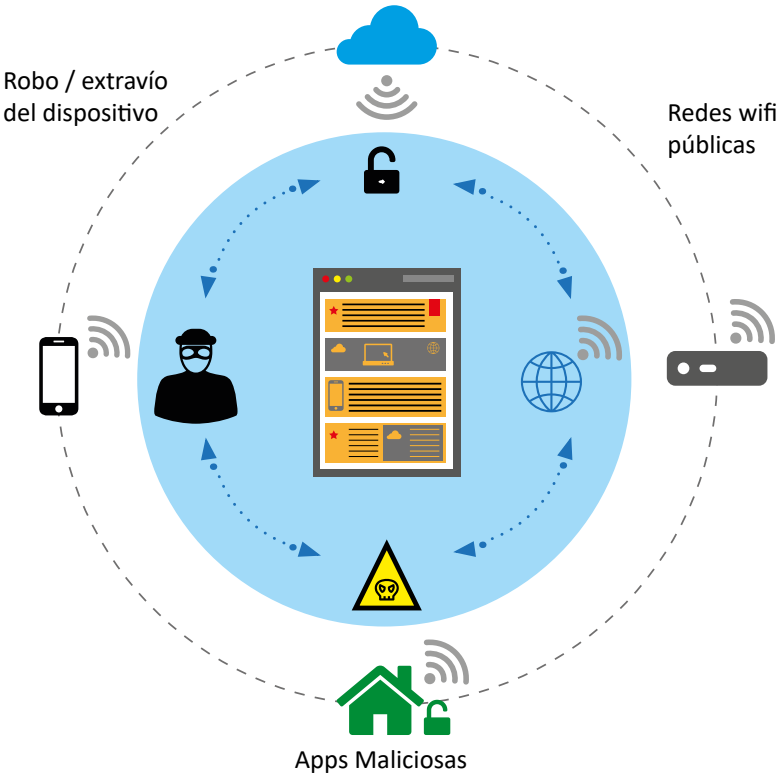
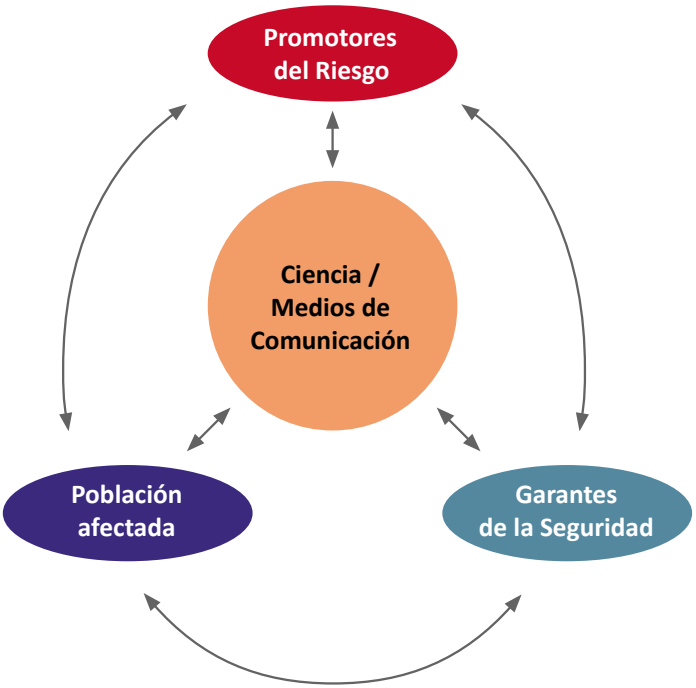


Ilustración 3. Seguridad en Internet. Dispositivos Móviles. Tomada de AEPD; INCIBE, ficha 1, p. 4

En una perspectiva diferente, Wynne (1998) sugirió considerar las dimensiones institucionales del riesgo, es decir, los juicios sobre las instituciones involucradas en la Gestión del Riesgo, su independencia, su legitimidad, su competencia y la justicia percibida en sus acciones, entre otras (pp. 57-58; Espugla Trenc, 2006, p. 83) En este esquema la definicion del riesgo tecnológico pasa por la interacción entre ciencia y medios de comunicación, toda vez que estos visibilizan las amenazas y juegan un rol de impulsadores, amplificadores o mitigadores (Espugla Trenc, 2006, p. 84). Adicionalmente, en términos teóricos se podría considerar un esquema básico de interacción entre tres actores: los promotores generadores del riesgo, la poblacion afectada y los encargados de garantizar la Seguridad.



Gráfica 5. Sistema de interacción de conflictos sociales relacionados con riesgos tecnológicos. Tomada de Espugla Trenc, 2006, p. 83

No obstante, es importante tener en cuenta que la red es un nuevo espacio donde los roles de los diferentes agentes se construyen, evolucionan y cambian día a día (Alonso García, 2015, p. 18; Pons Gamón, 2017, p. 81). El ciberespacio se ha convertido en una de las fuentes de importancia para los Estados más dinámica y cambiante y en uno de los ejes de atención político-militar más relevante de las relaciones interestatales. La popularización de Internet, no obstante, ha generado la eliminación de limitaciones en tiempo y espacio que dificultan las acciones encaminadas a determinar no solo amenazas potenciales sino a quienes perpetran los ataques.

A diferencia del mundo físico, donde los Estados tienen el monopolio legítimo de la violencia y los ataques son extremadamente costosos debido al alto costo de los recursos utilizados, el mundo cibernético permite superar estas limitaciones físicas asociadas al tiempo y el espacio, permitiendo acciones y ataques a bajo costo llevadas a cabo con gran precisión y efectividad (Gomes de Assis, 2017, p. 98).

Esta situación ha hecho que sea cada vez más relevante la Gestión del Riesgo desde un esquema de gobernanza internacional. La finalidad común de toda corporación multinacional como la gobernanza y la meta-gobernanza, es maximizar los entornos de Seguridad en los ámbitos político y económico, para lo cual se generan grupos de presión encargados de vigilar e impactar en las regulaciones internacionales y locales de los Estados (Reyes Beltrán, 2017, p. 59).

3. UNA PERSPECTIVA DE FUTURO

La soberanía de los Estados ha sufrido importantes modificaciones en el contexto de la globalización y a propósito de la desterritorialización favorecida por la emergencia de las nuevas tecnologías de la información, particularmente, con el auge de

las redes sociales. Las nuevas amenazas vinculadas a los Sistemas Ciberfísicos y el Internet de las Cosas -IoT, han presionado la necesidad de contar con un marco de comprensión común de seguridad y defensa del ciberespacio.

La sociedad del conocimiento, debido a un alto grado de incertidumbre frente a las amenazas tecnológicas, se ha visto de igual forma, abocada a establecer parámetros para la Gestión del Riesgo que se sobrepongan a la asimetría en el acceso y uso de la información y a la brecha tecnológica entre los países desarrollados y en vías de desarrollo. En esta vía, los avances de la Seguridad Digital han estado encaminados a fortalecer las capacidades de Defensa de los Estados con un mínimo de afectación en los derechos de los ciudadanos.

Aunque se ha reconocido el potencial de las nuevas Tecnologías de Información en aplicaciones de uso militar, las naciones se han comprometido con el respeto de los derechos humanos y las libertades fundamentales en el uso de las TIC (A/RES/71/28, 2016). Es así como organizaciones de carácter supranacional como la Organización de las Naciones Unidas -ONU, y la Organización para la Cooperación y el Desarrollo Económicos -OCDE, han proferido comunicaciones y recomendaciones encaminadas a mejorar la Seguridad de los Estados en materia digital, respetando la libertad de circulación y acceso a la información.

3.1. El Marco Internacional

En las últimas décadas se ha evidenciado la necesidad de continuar las investigaciones, el diseño de estrategias y la consolidación de las acciones encaminadas a combatir las amenazas que puedan afectar la Seguridad de los Estados. En esta medida, es importante considerar las nuevas Tecnologías de Información y Comunicación como herramientas que pueden ser empleadas con propósitos diferentes a mantener la estabilidad y la Seguridad internacional. Se trata de esta forma, de evitar que

las tecnologías digitales sean instrumentalizadas con objetivos delictivos o terroristas en detrimento de la Seguridad del Estado en las esferas civil y militar.

En el contexto de la Seguridad internacional y como respuesta a las amenazas potenciales a la Seguridad de los Estados, la comunidad internacional ha adoptado políticas orientadas por la Gestión del Riesgo en materia digital y tecnológica, con el propósito de salvaguardar la seguridad del ciberespacio. Entre otros, el fortalecimiento de la Seguridad Digital pasa por la consolidación de marcos jurídicos supranacionales y un sentido de la Defensa y la Seguridad Nacional. Asimismo, se ha considerado que el desarrollo tecnológico y digital es fundamental para el desarrollo de las economías y para la prosperidad social (OCDE, 2015, p. 415 y ss).

El flujo constante de información en el marco de la globalización y la revolución de la Tecnología de la Información y las Comunicaciones representó un cambio sustancial en la forma en que se conceptualizan y enfrentan los riesgos. El ataque del 11 de septiembre y la posterior respuesta contra el terrorismo configuró un entorno político mundial guiado por la constante amenaza de la violencia o de una guerra cuya duración y espacio no se pueden determinar con claridad. Esta imposibilidad de determinar el tiempo y espacio que ha de perdurar el conflicto se profundiza con la aparición de nuevas tecnologías y la expansión de un poder en red.

La OCDE ha señalado la necesidad de un sentido común en la comprensión de la Seguridad Digital y la responsabilidad compartida de los diferentes actores que pueden tener parte en su gestión. Esto ha hecho que la Organización recomiende para América Latina y el Caribe disponer de instrucción y capacidades para entender el riesgo y gestionarlo, atendiéndolo como un desafío económico y social y no solo como una cuestión técnica o de Seguridad Nacional (OCDE, 2015b).

La Organización de las Naciones Unidas, a través de la *Resolución 71/28*, sobre avances en la esfera de la información y las telecomunicaciones en el contexto de la Seguridad internacional exhortó a los Estados a promover en una escala multilateral, el examen de las amenazas reales y potenciales en la esfera de la Seguridad de la información y de posibles con el propósito de encararlas de manera compatible con la necesidad de preservar la libre circulación de la información y con el propósito ultimo de fortalecer la Seguridad de los sistemas mundiales de información y telecomunicaciones.

Para que la Estrategia de Gestión del Riesgo funcione, es necesaria la participación activa y comprometida de los diversos actores que se involucran en la gestión de los riesgos cibernéticos, comprendiendo empresas, sociedad civil, comunidad técnica de Internet y académicos, entre otros, en el desarrollo e implementación de estrategias y políticas públicas. De esta manera, se avanza, además, en el fomento de la cooperación internacional y la asistencia mutua, según la cual los responsables de políticas deben establecer relaciones multilaterales y bilaterales para compartir experiencias y buenas prácticas y promover un enfoque de Gestión del Riesgo de Seguridad Digital que no incremente el riesgo de otros países (OCDE, 2015b).

Desde esta perspectiva, el concepto de gobernanza se ha extendido, presentándose como una alternativa que favorece la articulación entre Estados y de estos con organizaciones no gubernamentales de diverso orden, en un entramado público/privado e inter-sistémico. La gobernanza permite asumir una mirada supranacional, considerando los diferentes actores que tienen lugar en los procesos contemporáneos a nivel internacional, regional y local (Reyes Beltrán, 2017, pp. 156-160).

Un ejemplo de esta forma de acción de acuerdo con los principios de la gobernanza internacional es la adopción por Organización de Estados Americanos de una Estrategia Intera-

mericana Integral de Seguridad Cibernética desde un enfoque multidimensional y multidisciplinario para la creación de una cultura de Seguridad cibernética. Como parte de esta estrategia se crea una Red Hemisférica de Equipos Nacionales de Respuesta a Incidentes de Seguridad de Computadores como un esfuerzo conjunto de los Estados Miembros y sus expertos para incrementar la Seguridad de las redes y sistemas de información con el propósito de abordar las vulnerabilidades y proteger a los usuarios, la Seguridad Nacional y las infraestructuras esenciales del Estado (AG/RES. 2004, 2004).

Esta necesidad de articulación ha sido reconocida por la ONU en la Resolución aprobada por la Asamblea General el 2 de diciembre de 2011. En ella se exhorta a los Estados a trabajar de forma articulada frente a las amenazas potenciales a la Seguridad Digital, promoviendo normas, reglas o principios de comportamiento responsable de los Estados y medidas de fomento de la confianza respecto del espacio informativo. (A/RES/66/24, 2011) Las recomendaciones de la ONU como de los paneles de expertos dispuestos por la organización señalan el camino para consolidar la seguridad tecnológica en el entendimiento de que las TIC son cimientos de la paz y la Seguridad internacionales (UNODA, 2018).

En un sentido similar, la *Decisión 587 de la Comunidad Andina*, adoptada el 10 de julio de 2004, establece los lineamientos de la Política de Seguridad Externa Común Andina, señalando dentro de los objetivos de dicha política prevenir, combatir y erradicar las nuevas amenazas a la Seguridad. En coherencia con esto, exhorta a los Estados miembros a actuar de manera conjunta a través de la cooperación y coordinación de acciones orientadas a enfrentar los desafíos que representan dichas amenazas para la Comunidad Andina.

El Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto

de la Seguridad Internacional encargado por la Organización de las Naciones Unidas, examina las amenazas reales y potenciales derivadas de la utilización de las TIC por los Estados y analiza las acciones necesarias para hacerles frente, incluidas normas, reglas, principios y medidas de fomento de la confianza.

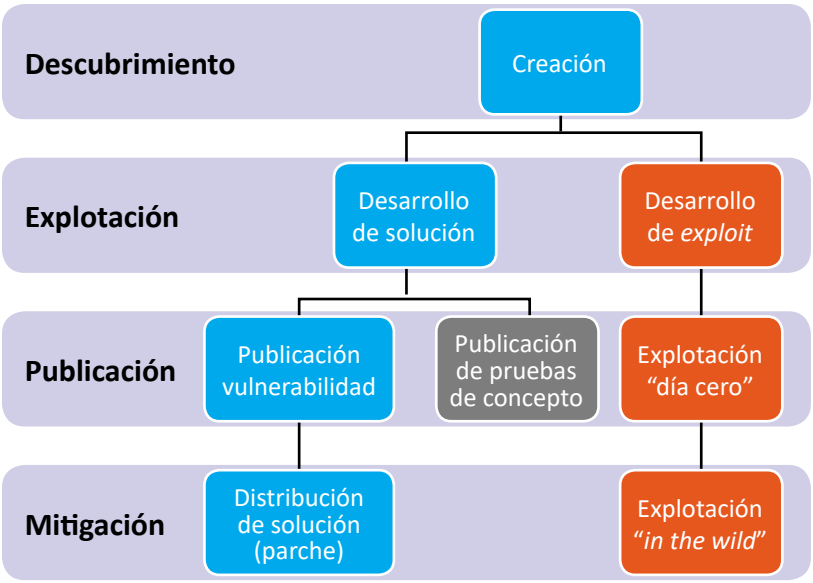


Ilustración 4. Ciclo de vida de las vulnerabilidades. Tomada de Escuela de Altos Estudios de la Defensa (2014, p. 32)

Es así como la gobernanza global permite la articulación del Estado con una pluralidad de organizaciones autónomas cuyas acciones son indispensables para el desarrollo de la pericia técnica y asesoramiento sobre la preparación de leyes, estrategias y marcos reguladores apropiados para hacer frente a las amenazas cibertecnológicas. Se trata de coordinar las acciones de diferentes entidades para producir y coordinar conjuntos de acciones que se consideran mutuamente benéficas.

3.2. El Marco del Estado

La cooperación internacional, sobre la base del mantenimiento de la Seguridad mutua, se establece de acuerdo con relaciones globales de carácter flexible. En este escenario y en el sentido que lo señalara Wynne (1998), la legitimidad de las instituciones y los métodos de creación, acceso y divulgación del conocimiento son fundamentales para evaluar el riesgo e identificar a sus principales impulsadores, amplificadores o mitigadores. Es así que la gobernanza puede entenderse como:

> […] la organización de la acción colectiva o la toma de decisiones colectivas que incluye mecanismos formales e informales para el uso de las reglas, todo ello coordinado por una gran variedad de actores estatales y no estatales (Haufler, 2006; Neiva Santos, 2009, pp. 49-53; Reyes Beltrán, 2017, p. 59).

El concepto de gobernanza ha permitido situar al Estado como instancia coordinadora entre otros muchos actores globales, sobreponiéndose a la desconfianza en las instituciones y decisiones del orden nacional y una sociedad en red erosionada. De esta forma, la gobernanza permite ir más allá de los límites del Estado frente a asuntos en los no puede intervenir, empleando para ello un modelo de gobierno basado en la evaluación, control y gestión democrática de los riesgos, cuyo propósito final es intervenir para conciliar los intereses, preferencias y objetivos científicos, políticos, económicos y sociales (Rivera Berrío, 2009, p. 2).

La premisa primordial que orienta las acciones de los Estados en materia de Ciberdefensa es que la gravedad de las amenazas a la Seguridad cibernética para la Seguridad de los sistemas de información esenciales, las infraestructuras esenciales y las economías en todo el mundo, requieren de acciones eficaces para abordar estas problemáticas, por lo que se debe contar con

la cooperación intersectorial y la coordinación entre una amplia gama de entidades gubernamentales y no gubernamentales (AG/RES. 2004, 2004).

> Según lo anterior, la globalización como proceso estructural ha creado una interdependencia global entre las organizaciones e instituciones en diferentes ambientes funcionales, como la economía y la política, que afectan de forma diferente los diferentes espacios nacionales o locales, originando jerarquías complejas que se desarrollan de forma desigual en el espacio-tiempo, y genera una infinidad de variables dispersas de un amplio alcance espacial (Reyes Beltrán, 2017, p. 157).

El desarrollo de la sociedad del conocimiento se une a la concepción de fomento del desarrollo humano en el que la responsabilidad de los Estados en cuanto a la inversión en ciencia y tecnología es fundamental para disminuir la desigualdad. "El objetivo del desarrollo mediante la innovación exige también la instauración de incentivos financieros" (Unesco, 2005, p. 161). Así mismo, la toma de conciencia sobre riesgos globales y la posibilidad de interconexión en escalas sin precedentes, han fomentado las capacidades de movilización y organización transnacional, ofreciendo la posibilidad de generar una democracia prospectiva acorde con los lineamientos de un gobierno abierto y transparente (Unesco, 2005, pp. 201-202).

Las libertades de opinión, expresión e información, en un Estado democrático, deben favorecer la expresión de opiniones de cualquier índole y la búsqueda, acceso y difusión de la información sin restricciones. El fomento de estas libertades en los Estados debe reconocer y gestionar adecuadamente al menos tres dimensiones, a saber, las posibilidades tecnológicas para que fluya la información, la libertad individual para acceder a ella y el riesgo de que personas ajenas invadan la intimidad y la

privacidad de los individuos (Valle, 2003, p. 48).

Es así como la posibilidad de administrar la Seguridad Digital debe contemplar tanto los aspectos tecnológicos propios de esta tarea, como la Ley de Seguridad, la Seguridad Nacional y la Defensa de los intereses de los Estados y los ciudadanos. Los retos que imponen una acción de esta magnitud son fundamentales para la economía y la prosperidad social por lo que debe contemplar así mismo, una cultura digital de protección desde el ámbito micro (individuos) hasta el supranacional., de forma coherente con los resultados de la aplicación las herramientas de evaluación y una visión general de la política de política pública.

3.3. En Colombia

En este sentido, la *Ley 1288 de 2009*, declarada inexequible por la Corte Constitucional, es un ejemplo de que los requerimientos de las agencias de Iinteligencia y las normas de una sociedad abierta plantean dilemas para el gobierno democrático. En el *Artículo 2* del primer capítulo, la Ley enuncia,

> La función de Inteligencia y Contrainteligencia es aquella que se desarrolla por organismos especializados del Estado, del orden nacional, dedicados al planeamiento, recolección, procesamiento, análisis y difusión de la información necesaria para defender los derechos humanos, prevenir y combatir amenazas, internas o externas, contra la convivencia democrática, la seguridad y la defensa nacional, y demás fines enunciados en esta ley.

Sin embargo, la Corte en los pronunciamientos *C-567 de 1997*, *T-729 de 2002*, *C-993 de 2004* y *C-981 de 2005*, alegan que en cuanto el derecho a la autodeterminación informática o *hábeas data* consiste en las facultades de conocer, actualizar y

rectificar la información personal contenida en bases de datos, y que la forma como estas últimas sean configuradas y administradas delimita el ámbito de aplicación de las facultades que componen el objeto de ese derecho.

> Así mismo, la sentencia C-913 de 2010, establece que
>
> En lo atinente a los apartes acusados del artículo 16, explican que este asigna al Gobierno Nacional la competencia para reglamentar los procedimientos de acceso a esta información por parte de los miembros de la Comisión Legal Parlamentaria de Seguimiento a las Actividades de Inteligencia y Contrainteligencia, lo que tampoco sería constitucionalmente factible, al recordar que lo relativo al acceso a la información contenida en bases de datos es un tema que debe ser regulado únicamente por leyes estatutarias.

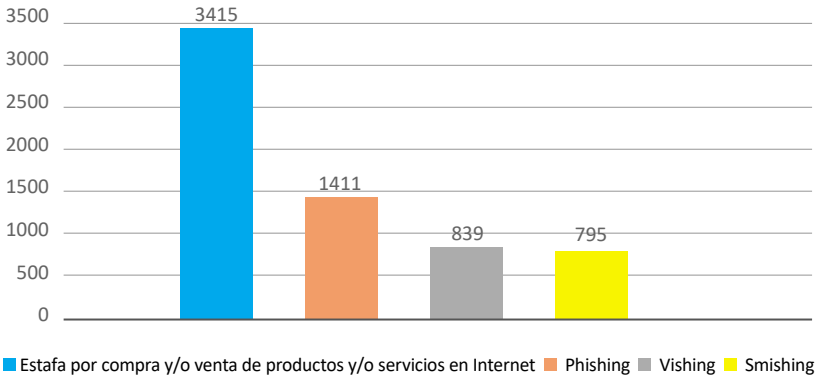
No obstante, en los últimos años se ha presentado un progreso importante frente al desarrollo y aplicación de las Tecnologías de la Información y las Comunicaciones, así como en las acciones encaminadas a consolidar la Seguridad y la Defensa en este ámbito. Un avance en este aspecto, luego de que la *Ley 1288 de 2009* fuera declarada inexequible por la Corte Constitucional, es la promulgación de la *Ley 1273 de 2009* por medio de la cual se está creando un nuevo bien jurídico tutelado denominado protección de la información y de los datos orientada hacia la preservación de los sistemas tecnológicos y los derechos de los ciudadanos.

La *Ley 1273 de 2009* crea el marco jurídico a partir del cual en Colombia se hace posible penalizar conductas como el acceso abusivo a un sistema informático, la obstaculización ilegítima de sistema informático o red de telecomunicación, la interceptación de datos informáticos, el daño informático, uso de software malicioso, la violación de datos personales y

la suplantación de sitios web para capturar datos personales (p. Cap. 1).

De esta manera, la *Ley 1273* responde a los principales problemas cibernéticos que enfrenta el país, aquellos que tienen que ver con los campos comerciales y financieros. Generalmente, los ciudadanos son quienes más reportan eventos con un 66 % de los incidentes, debido a falsas ofertas (*phishing*) publicadas en portales web e incluso reconocidas tiendas de comercio electrónico como mercadolibre.com, OLX.com, tucarro.com.

Las estafas por *vishing* y *smishing*, corresponden a la difusión del mensaje y posterior llamada del delincuente. Una de las modalidades más empleados son los anuncios de premios por parte de operadores de telefonía celular y almacenes de cadena, las falsas ofertas en bolsas de empleo virtuales y la falsa llamada que asegura tener información sobre un sobrino retenido. En este panorama, el Internet de las cosas representa uno de los mayores retos para el gobierno colombiano debido al incremento de usuarios y dispositivos conectados con una cifra que se espera llegue a los 25 mil millones de dispositivos conectados a Internet para el 2020 (Policía Nacional, 2017, p. 12).



Gráfica 6. Ciberestafa en Colombia, 2016 – 2017. Tomada de Policía Nacional, 2017, p. 4

Las estrategias de Ciberdefensa y Ciberseguridad se han desarrollado, además, a partir del *Conpes 3701 de 2011*, en donde se plantean tres pilares fundamentales, la adopción de un marco interinstitucional apropiado para prevenir, coordinar, controlar y generar recomendaciones para afrontar las amenazas y los riesgos que se presenten; el desarrollo de programas de capacitación y formación especializada en Seguridad de la información; y, el fortalecimiento de la legislación nacional y la cooperación internacional en estas materias (A/69/112, 2014, p. 7).

Colombia integra el Comité Interamericano contra el Terrorismo, CICTE de la Organización de los Estados Americanos, OEA, que tiene como propósito principal promover y desarrollar la cooperación entre los Estados Miembros para prevenir, combatir y eliminar el terrorismo. (OEA, 2018) Como parte del CICTE, el país ha logrado trabajar con varios equipos de respuesta ante incidencias de Seguridad, CSIRT en la región, proporciona formación técnica a personal especializado, promueve el desarrollo de estrategias nacionales sobre seguridad cibernética, y fomenta el desarrollo de una cultura que permita su fortalecimiento en el continente (Conpes 3854, 2016, p. 15).

Como parte de las estrategias de combate contra las amenazas al ciberespacio y en el marco de la cooperación internacional y las acciones conjuntas entre los Estados, el Centro Cibernético Policial colombiano (2018) ha enfocado sus esfuerzos en la Gestión del Riesgo orientada no solo hacia la contención de las amenazas sino también hacia su prevención. En este marco el Centro Cibernético Policial adelanta campañas de concientización, sensibilización y educación de los riesgos de Seguridad Digital, en coherencia con las recomendaciones del Consejo mundial de la industria de tecnologías de la información (ITI por sus siglas en inglés).

Asimismo, la política nacional de Seguridad Digital consagrada en el *Conpes 3854 de 2016*, adopta una visión de la ges-

tión sistemática y cíclica del riesgo, según la cual se define un objetivo o el diseño de una actividad, se evalúa cuál es el nivel de riesgo de dicha actividad determinando todos los resultados posibles de asumirlo sobre los objetivos sociales y económicos y se determina cómo debería ser modificado el mismo (Conpes 3854, 2016, p. 26).

Esta gestión sistemática y cíclica del riesgo es liderada desde el alto nivel del gobierno en favor de la Defensa y Seguridad Nacional para estimular la prosperidad económica y social en coherencia con los lineamientos de la OCDE. Adicionalmente, se adopta un enfoque multidimensional que incorpora tanto los aspectos técnicos y jurídicos como lo económico y lo social y a los diversos actores involucrados promoviendo la responsabilidad compartida en coherencia con los lineamientos de la ONU (Conpes 3854, 2016, p. 27).

De esta manera, el *Conpes 3701 de 2011*, concentró los esfuerzos del país en contrarrestar el incremento de las amenazas informáticas que lo afectaban significativamente, y en desarrollar un marco normativo e institucional para afrontar retos en aspectos de Seguridad cibernética. El *Conpes 3854 de 2016*, por su parte, avanzo en el fortalecimiento del Estado frente a las amenazas en el ámbito cibernético comprendiendo la Ciberseguridad y la Ciberdefensa Nacional adoptando el enfoque de prevención y Gestión del Riesgo.

> En el ámbito regional, Colombia se ha posicionado como uno de los países que más ha avanzado en aspectos relacionados con Ciberseguridad y Ciberdefensa. Lo anterior, se refleja en indicadores de eficiencia comparativa como el Índice Mundial de Ciberseguridad de la Unión Internacional de Telecomunicaciones (UIT). Según este, en 2014 el país se ubicaba en el quinto lugar del ranking a nivel regional, siendo superado por Estados Unidos, Canadá, Brasil y Uruguay;

mientras que en el plano mundial comparte la novena posición, junto con países como Dinamarca, Egipto, Francia y España (Conpes 3854, 2016, p. 16).

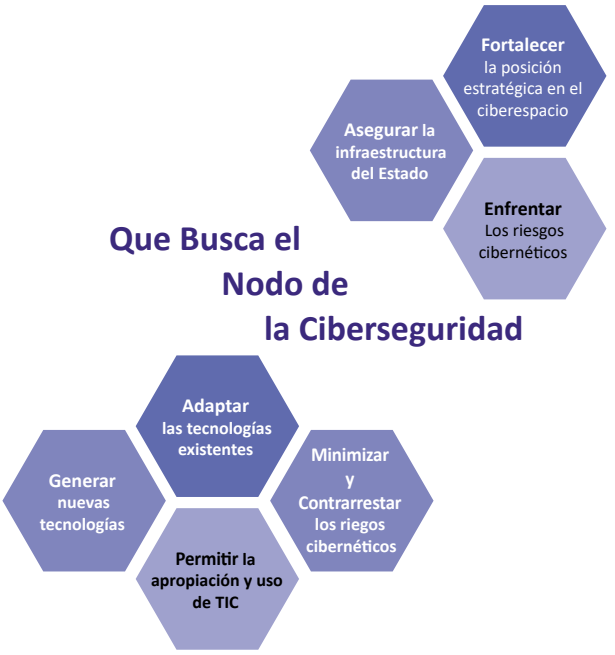


Ilustración 5. Nodo de Ciberseguridad. Elaboración propia a partir de MinTIC (2018)

Los esfuerzos de país en cuanto a la cooperación internacional de lucha contra el cibercrimen han avanzado en torno a la noción de gobernanza, entendiendo esta como la acción del gobierno en la coordinación y gestión de redes en las que participan multiplicidad de actores públicos y privado. Desde esta perspectiva se han desarrollado grupos nacionales de alerta, vigilancia y prevención que contribuyen al desarrollo de estrategias nacionales sobre Ciberseguridad en la región y en el mundo, y ha participado en Congresos sobre el manejo de incidentes relacionados con la Seguridad de la información y el delito cibernético. (A/69/112, 2014).

En este mismo marco, Colombia ha establecido los vectores de desarrollo, directrices marco, orientadas a fortalecer la posición del país en términos de Ciberseguridad, alineados con las diferentes estrategias nacionales provenientes desde las entidades del Estado y del sector privado. De esta manera el Estado colombiano ha afrontado una mayor articulación para prevenir, controlar y manejar las consecuencias de la complejización del mundo en la fase de la globalización.

La Gestión del Riesgo y la cooperación internacional en materia de Ciberseguridad se complementa con procesos de innovación orientados a la generación de soluciones en TIC, con lo que se pretende fomentar las capacidades de los ciudadanos y el Estado para buscar, identificar, estructurar, analizar, recuperar, correlacionar y/o integrar datos relacionados con las incidencias de naturaleza cibernética (MinTIC, 2014, pp. 5 – 10).

Conclusiones

Las tecnologías de información y comunicación ofrecen oportunidades de interacción y articulación sin precedentes, pero en la misma medida plantea retos, debilidades y amenazas para los Estados y los ciudadanos. La ciberguerra y el cibercrimen son en este contexto, peligros que ponen en riesgo la infraestructura de los Estados, haciendo cada vez más importante aumentar la resiliencia cibernética, llegar a un acuerdo sobre leyes y normas que se apliquen a la utilización de las tecnologías de la información y las comunicaciones y participar en medidas de fomento de la confianza (A/69/112, 2014, pp. 2-3).

Dado el carácter dinámico de las tecnologías y su acelerado ritmo de cambio, el ciberespacio presenta limitaciones para los Estados debido a la dificultad para establecer el origen de las amenazas y su autoría. De allí que sea necesario avanzar en estrategias que no solo contemplen los aspectos técnicos de las amenazas tecnológicas sino su dimensión social, trascendiendo

la visión de la Ciberseguridad hacia una de la innovación tal y como ha sucedido en el Estado colombiano.

La innovación y el fomento de la ciencia y la tecnología, permite avanzar en el fortalecimiento de habilidades y capacidades para el descubrimiento diario de nuevas vulnerabilidades en el *software* y *hardware*. El número de incidentes relacionados con ciberataques no parece disminuir en el corto plazo, por el contrario, las proyecciones en hacia el año 2020 indican un incremento acelerado de los dispositivos y usuarios de Internet y dispositivos móviles, incrementando a su vez las amenazas y los riesgos.

Los Estados se han venido preparando para afrontar este contexto en materia de Seguridad cibernética, siendo Colombia un caso representativo en la región, manteniendo un suministro constante y fiable de información sobre amenazas y vulnerabilidades en el ciberespacio y determinando las acciones que le permiten responder ante estos incidentes y recuperarse de los mismos, en coherencia con las recomendaciones y acciones de organizaciones supranacionales como la ONU, OEA, OCDE y la Comunidad Andina de Naciones.

Los piratas informáticos, los grupos delictivos organizados y los terroristas que emplean la Internet para fines ilícitos, representan amenazas no solo para la infraestructura de los Estados sino también, para la prosperidad social y económica de sus ciudadanos. Impiden el crecimiento y desarrollo de las nuevas Tecnologías de Información y Comunicación al fomentar el temor frente a medios inseguros y poco confiables para realizar transacciones personales, gubernamentales o de negocios.

En esta medida, se hace necesario continuar en el fortalecimiento de marcos jurídicos nacionales y supranacionales, que sin limitar o afectar las libertades de los usuarios relacionadas con el acceso y difusión de la información, establezca con ma-

yor precisión las características y límites del ciberespacio y las posibilidades de acciones delictivas en él. Una estrategia de este tipo requiere, además, continuar trabajando en los esfuerzos de articulación entre los Estados y de estos con usuarios y actores privados con posibilidad de acceder a Internet.

Sin duda, la Gestión del Riesgo y la gobernanza representan dos de las herramientas más importantes para el fortalecimiento de las capacidades de los Estados en materia de Ciberseguridad y Ciberdefensa. Estas permiten el abordaje cíclico y sistémico de las amenazas y proveen las posibilidades de cooperación que hace posible mantener un flujo de información constante y necesario para afrontar amenazas cambiantes que comportan un alto grado de incertidumbre. Estas herramientas y las relaciones que se posibilitan a partir de allí representarán en el horizonte 2020 un nuevo campo para las prácticas de la Inteligencia estatal.

CAPITULO III

EL IMPACTO DE LA ACADEMIA EN LA CIBERSEGURIDAD[13]

Alejandro Bohórquez-Keeney[14]
Escuela Superior de Guerra

1. INTRODUCCIÓN: ACADEMIA Y SEGURIDAD

La aparición del ciberespacio ha alterado todos los espacios de la vida cotidiana, llevando así a transformaciones importantes en las instituciones sociales, políticas y de Seguridad, llegándosele a considerar hoy en día como el quinto campo estratégico. Precisamente, esta particularidad del ciberespacio de permear todos los sectores sociales hace que ninguna institución pueda abstraerse de este, en particular de las amenazas que provienen del campo estratégico artificial. De ahí, la importancia de que el sector académico haga presencia en los programas y las políticas públicas que aborden la Ciberseguridad.

De entrada, la educación es considerada como servicio esencial para el mantenimiento de las funciones sociales básicas del

13 Capítulo de libro resultado del proyecto de investigación titulado "Gestión de Riesgos en Seguridad Digital" de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra, que a su vez hace parte de la línea de investigación 'Seguridad Digital' del grupo de investigación 'Masa Crítica', reconocido y categorizado en (C) por Colciencias. Registrado con el código COL0123247, está adscrito a la Escuela Superior de Guerra de la República de Colombia.

14 Profesional en Política y Relaciones Internacionales (Universidad Sergio Arboleda), Magister en Inteligencia Estratégica (Escuela de Inteligencia y Contrainteligencia). Docente, Investigador de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto". Patrocinado por el Patrocinado por el Ministerio de Tecnologías de la información y las comunicaciones.

Estado, y por ello hace parte de la infraestructura informática crítica de Colombia (CCOC, 2015). Al recordar que parte de lo que constituye la Infraestructura Informática Crítica es un nivel material donde se encuentran los servidores, conexiones, satélites y aparatos que son utilizados para acceder al ciberespacio, a la vez de un nivel inmaterial que corresponde a la información almacenada y distribuida por dicha infraestructura (Dunn & Suter, 2012). Por tales motivos, el sector académico es clave teniendo en cuenta que dentro de las universidades se encuentra un importante componente de la infraestructura física del ciberespacio, como también la importancia de la información que se maneja en las instituciones académicas. Adicionalmente, por su función social es al sector académico al que le correspondería la capacitación y entrenamiento en cuestiones de Ciberseguridad.

En el presente capítulo, se examinará el estado de la cuestión pertinente al papel desempeñado por la academia dentro de la Seguridad Digital. En primer lugar, se revisarán las principales políticas públicas en materia de Ciberseguridad dentro de la región, al igual que de otros países de interés, haciendo un énfasis particular en el papel que desempeña el sector Educación dentro de ellas. Esto con el fin de entender cómo han sido las concepciones que se tiene de este sector como parte fundamental de la Infraestructura Informática Crítica. En principio, se tomarán en cuenta los actores regionales que por su relevancia vale la pena considerar, para luego mirar casos de interés en el hemisferio norte.

En segundo lugar, se revisarán los documentos académicos que hagan mención directa, o que se aproximen de manera suficiente, a los acercamientos que ha hecho la academia en su papel definido dentro de la Infraestructura Informática Crítica. Para poder lograr este perfilamiento del sector académico, se tomarán en cuenta los resultados que arroje la revisión hecha en el aparte anterior, sumado al resultado de las mesas de trabajo realizadas por la Maestría de Ciberseguridad y Ciberdefensa

frente al tema de la Gestión de Riesgos en Seguridad Digital. El eje central de esta segunda revisión es la ejecución de las políticas públicas en Seguridad Digital, y cómo se han llevado a cabo hasta el momento, de ahí, la necesidad de perfilar primero el rol de la academia en este campo.

En tercer lugar, se hará una nueva revisión documental, pero en este caso se basará en la proyección a futuro que se hace del sector académico en el ámbito de la Ciberseguridad. De este modo, se busca visibilizar las posibles fortalezas que se esperan desarrollar, así como los futuros retos que pueden aparecer, entendiendo que la complejidad del ciberespacio hace que este sea un entorno altamente variable. Así las cosas, puede hacerse un balance más definido y detallado de la importancia del sector académico como actor primordial de la Ciberseguridad de un Estado, y en particular, Colombia.

Finalmente, se presentarán unas conclusiones donde se relacionan todos los hallazgos encontrados en esta investigación, y aportar de esta manera, posibles escenarios y recomendaciones frente al tema propuesto. Por ende, este capítulo busca ir más allá de una mera recopilación documental, y ser propositivo para nuevas investigaciones y proyectos relacionados con la Seguridad Digital, y más con la academia como actor principal.

2. POLÍTICAS PÚBLICAS, ACADEMIA Y SEGURIDAD DIGITAL

Como se mencionó en la introducción, en este aparte se hará una revisión de las políticas públicas en Ciberseguridad, y cuál es el papel y las funciones que estas le otorgan al sector académico a desempeñar en este campo. Por un lado, se tomarán en consideración las políticas de los principales actores de la región, debido a que su proximidad con Colombia los hace principales socios estratégicos en caso de lograrse tratados regiona-

les sobre Seguridad Digital, además de las posibles lecciones a aprender de ellos. Por otro lado, se revisarán las políticas elaboradas por los países líderes en el tema de Ciberseguridad, cuyo acceso sea abierto a la revisión por parte de personal externo a sus entidades estatales.

Antes de continuar, vale aclarar que de acuerdo con el Banco Interamericano de Desarrollo (BID), existe una falta de conciencia en la región sobre la Ciberseguridad, a causa de una ausencia por parte del sector académico en este tema. Puntualmente, "pocos países ofrecen programas de educación a nivel posgrado para la Seguridad cibernética, y los programas de formación profesional son más comunes, pero varían en calidad" (Foro Económico Mundial, 2016, p. 26). Esto, ya denota los grandes vacíos y los grandes retos que afronta el sector académico, no solo en Colombia, sino también en la región, al no apropiarse de un tema que como se mencionó le es vital. A causa de esto, para conocer cómo el tema de la Ciberseguridad afecta la academia, es que se toma esta revisión de políticas públicas.

Inicialmente, aquí en Colombia el *Conpes 3854 de 2016* enfatiza el sector Educación como parte de la Infraestructura Informática Crítica, y como una de las múltiples partes interesadas que dependen del entorno digital para su buen funcionamiento. De hecho, de acuerdo con este documento la educación y el aprendizaje ocupan un 36.7 % de la actividad ciberespacial nacional (Conpes 3854 de 2016), lo que resalta la importancia de este sector dentro del entorno digital colombiano. Aun así, el papel que se le asigna a este sector se limita a la capacitación y difusión de buenas prácticas, sin que se le determinen acciones más proactivas en materia de Ciberseguridad.

Igualmente, en su Política Nacional de Seguridad advierte la necesidad de la participación activa de su respectivo sector académico, pone como labor principal de este, la formación en buenas prácticas cibernéticas. De manera similar al *Conpes 3854*

(2016), la política chilena de Ciberseguridad aborda este reto desde todos los niveles educativos, subrayando la necesidad de la instrucción de dichas prácticas desde una edad temprana. De esta forma, son claros y particulares a los retos y desafíos a los que se enfrenta el sector académico del país austral.

De manera análoga y muy similar, México (2017) en su Estrategia Nacional de Ciberseguridad ubica también al sector académico como jugador clave y capacitador en materia de su propia Seguridad informática. Esta estrategia, es bastante insistente en la idea de establecer acciones coordinadas entre el sector académico y demás partes interesadas (México, 2017), aunque no establece planes de acción claros y su contenido sigue siendo muy general. En este instante, ya se puede ir adelantando una conclusión respecto a la participación del sector académico en la Ciberseguridad, y es que su papel se define más desde la participación que desde la acción.

Por su parte, Brasil presenta un caso interesante para las políticas de Ciberseguridad, al no contar con una sino con tres de ellas en su proyección de liderazgo regional, siendo estas: la *Política Cibernética de Defesa* y la *Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal* (2015-2018) (Cruz Lobato, 2017). La primera de ellas, se concentra exclusivamente en Ciberdefensa, y por este motivo es de alcance exclusivamente militar (Estado-Maior Conjunto das Forças Armadas, 2014); en cambio la segunda, la academia, es identificada como sector estratégico de la Ciberseguridad, y se establece como prioridad su cooperación y creación de redes de información con este (Departamento de Segurança da Informação e Comunicações, 2015). A diferencia de las políticas referenciadas anteriormente, no hace explícita la necesidad de que el sector académico se encargue de la capacitación y formación de expertos en Ciberseguridad, o de buenas prácticas digitales.

En el caso peruano, se trata de una política de Ciberseguridad muy incipiente que apenas contempla al sector académico como parte interesada en este campo, mas no presenta un curso de acción específico (Secretaría de Gobierno Digital, 2017). Ni qué decir, de lo que sucede en Argentina, donde existe una normatividad sobre Seguridad pero no una política pública como tal (Gobierno de Argentina, 2018), y a pesar de contar con el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC), a la fecha que esto se escribe, aún está en sus planes desarrollar una política pública en Ciberseguridad (ICIC, 2018). Así entonces, se revela que el desarrollo en Ciberseguridad dentro de la región es aún muy precario, y de ahí parte la dificultad de rastrear programas específicos para el sector académico en este campo.

Ahora bien, llevando la mirada al hemisferio norte se pueden encontrar varios casos que son de interés en materia de Ciberseguridad, y de los cuales se podrían esperar aportes importantes para el sector académico. Para realizar esta revisión de una manera que no sea aleatoria, se toman nuevamente como base las recomendaciones del BID, que califica como los Estados más avanzados en materia de Ciberseguridad a Estados Unidos de América, Estonia, Israel y Corea del Sur (Lewis, 2016). Debido a limitaciones idiomáticas, además de tratarse de países que tienen un tratamiento muy hermético de sus documentos, se debe descartar a Rusia y a China para esta revisión.

Como es de esperarse, los Estados Unidos de América presentan una Estrategia de Ciberseguridad que presenta unos lineamientos generales, que además abarca el tema de alianzas internacionales, y al sector académico lo sitúa en el papel de capacitación (Department of Defense, 2015). No obstante, lo interesante en este caso es cómo existen políticas complementarias que abordan la intersectorialidad de la Ciberseguridad, incluso provenientes de otros departamentos; ya en el caso del sector académico está la *National Initiative for Cybersecurity*

Education (NICE) Cybersecurity Workforce Framework del Departamento de Comercio, en la cual se estipulan las tareas, herramientas y capacidades que se deben desarrollar en pro de este objetivo (Newhouse et al., 2017). Para futuras revisiones, y dado el carácter nacional de este país, se requiere una revisión de las políticas privadas en esta materia y en este sector.

Por otra parte, como es sabido, Estonia fue víctima de uno de los mayores ataques cibernéticos registrados, y por tal motivo la Ciberseguridad es prioritaria en su Estrategia Nacional, haciéndola líder en la Unión Europea (Carr, 2011). A raíz de esto, y dada la naturaleza soterrada del ciberespacio, una de las particularidades de la política pública estonia es que tiene una versión pública y otra clasificada; de la primera, parte otra particularidad en que el ministerio encargado de centralizar y coordinar la Estrategia de Ciberseguridad en Estonia es el Ministerio de Asuntos Económicos y Comunicaciones, y no el Ministerio de Defensa (Ministry of Economic Affairs and Communication, 2014). Sin embargo, aunque reconocen la necesidad de la participación del sector académico, abiertamente no se le asignan mayores tareas, aunque en este caso la capacitación se da a nivel local e internacional dada la experiencia estonia (Pernik & Tuohy, 2016).

Al observar el caso de Israel, dentro de su política de Ciberseguridad presenta un programa educativo específico liderado por el propio Ministerio de Educación, el *Magshimim*, que además involucra a el IDF, la Oficina del Primer Ministro, la Agencia de Seguridad Israelí, el *Mossad*, la Lotería Estatal Israelí y la Fundación *Rashi* (Housen-Couriel, 2017). Este programa se adoptó como política nacional a partir de 2013 luego de una prueba piloto de dos años, y busca instruir a los estudiantes de últimos años de bachillerato que demuestren aptitudes informáticas y buen desempeño académico para servir en las unidades tecnológicas del IDF (Rashi Foundation, 2018). Entonces, se evidencia aquí cómo el tema de prevención temprana toma un nuevo

cariz, y la necesidad de actuar en sinergia con los estamentos de seguridad del Estado para así lograr mejores resultados.

Finalmente, Corea del Sur más que aplicar una política de Ciberseguridad, ha diseñado todo un libro blanco aplicado al Internet específicamente. Lo novedoso y realmente diferenciador de este documento, es el hecho de que cubre desde la academia la necesidad de impartir una ética del Internet, al cual contempla principalmente protección a menores, y lo hace con programas lúdicos que lleguen a esa población (s.a., 2015). Por ende, los aportes que se pueden dar desde el sector académico van más allá de considerar exclusivamente la capacitación técnica, y requieren del aporte de otros campos de estudio.

Luego de revisar todos estos casos, es claro que al sector académico aún le queda mucho por abarcar en materia de Ciberseguridad, como agente proactivo y parte interesada en el desarrollo de este campo. Si bien el sector académico por principio debe encargarse de la capacitación de los agentes de Ciberseguridad, como lo demostraron los documentos revisados, también tiene el deber de educar en el buen uso del Internet y los componentes éticos alrededor de este, y desde edades tempranas. De todos modos, queda aún por explorar al sector académico como agente activo en la prevención de ciberataques, dada su participación dentro del ciberespacio, y los nuevos retos que puedan ir surgiendo en el futuro.

3. LA ACADEMIA FRENTE A LA SEGURIDAD DIGITAL

En cuanto a la ejecución del papel de la academia como capacitador en Seguridad Digital, es interesante notar cómo este lleva a un amplio rango de aspectos que abarcan todos los sectores de la sociedad, conduciendo a un vasto número de publicaciones en Seguridad Digital. Por esta razón, es que hizo una

revisión desde los principales motores de búsqueda de artículos académicos como Scopus, Wiley o Google Scholar para clasificar en categorías amplias los artículos académicos existentes que aborden el tema de Seguridad Digital. Por consiguiente, en este aparte se hará un esbozo de cómo la academia cumple con su papel de capacitador en Seguridad Digital, y las lecciones que se puedan aprender de estos casos.

Antes de continuar, es pertinente traer a colación los resultados de las mesas de trabajo para la identificación a través de las múltiples partes interesadas de las líneas de investigación en Gestión de Riesgos en Seguridad Digital, desarrolladas en conjunto por MinTIC y la Escuela Superior de Guerra el 26 de abril de 2018. En ellas, dentro de la mesa específica al sector académico se reafirmó una vez más que el papel que debe desempeñar dicho sector es el de capacitador, agregando además la necesidad de crear un centro de innovación en Seguridad Digital, como también la creación de una red académica en esta materia (Bohórquez-Keeney, 2018). Así, observando esto, el alcance de la academia en Seguridad Digital va más allá de la instrucción formal y busca ampliar su acceso de manera multisectorial.

Si bien esas fueron las conclusiones principales de las mesas de trabajo, no se pueden echar en saco roto las demás propuestas presentadas dentro de su realización, puesto que son propuestas de las que se alimentan los artículos académicos reseñados más adelante. En ese orden de ideas, entre las temáticas relevantes avanzadas en la actividad están: Internet de las Cosas, Infraestructura Informática Crítica, Ciberinteligencia y Ética digital (Bohórquez-Keeney, 2018). De tal modo, estas cuatro temáticas serán los ítems a revisar en esta parte del estado de la cuestión, y así empezar a evidenciar los avances de la academia como capacitador en Seguridad Digital.

Al iniciar a un nivel general, es rescatable la publicación hecha por la Escuela Superior de Guerra “Geeneral Rafael Re-

yes Prieto", acerca del ciberespacio a cargo de Andrés Gaitán (2012), en el cual se hace un abordaje general del quinto dominio estratégico. Por supuesto, al ser una producción desde las ciencias militares su enfoque está encuadrado en el tema de ciberguerra, y los alcances que esta ha tenido hasta la fecha de publicación del texto. Este es un referente importante, al tratarse de uno de los primeros textos en Colombia que abordan al ciberespacio, y lo referente a la Seguridad dentro de este, desde una perspectiva académica.

De igual manera, no se deben descartar los avances académicos hechos sobre el papel central del sector académico en el tema de Seguridad Digital, que se estableció anteriormente, es decir, la capacitación en Seguridad Digital. Bajo esta línea se encuentran trabajos como el presentado por Jiménez *et al*. (2014), en el cual no solo se hace énfasis en la capacitación en Seguridad Digital, sino que lo hace en la necesidad específica que tiene la academia en apropiarse de estas herramientas, al hacer un estudio de caso en los planteles de educación básica y media en Sogamoso, Boyacá. También relevantes, son los artículos en capacitación académica que abogan por una mayor cercanía entre el sector público y el privado, teniendo en cuenta el alcance que debe tener la Seguridad Digital, tal como lo argumentan Acosta y Martínez (2017).

Así, entrando ya en los ítems propuestos, una tendencia relevante que se está dando en la actualidad es el *Internet of Things* o Internet de las Cosas, entendido como "el concepto de que todo puede ser enlazado a un aparato conectado a la red para recolectar o hacer uso de datos" En primera instancia, están aquellos documentos que dan una visión general sobre la seguridad en el Internet de las Cosas, así, trabajos como el de Huang *et al*. (2016) investigan las posibles vulnerabilidades dentro de estas redes, y las formas de mitigarlas, o como los de Roman *et al*. (2013) que dan cuenta del alcance multidimensional de este nuevo fenómeno cibernético. Consecuentemente, existen también textos muy

completos como el presentado por Tejero (2017), proveyendo metodologías específicas de Seguridad en casos puntuales.

Por otra parte, la Seguridad en el Internet de las Cosas no se limita exclusivamente a temas técnicos o de ingeniería, debido a su alcance también es un campo fértil para el derecho, las ciencias jurídicas y la ciencia política, campos de conocimiento que tienen algo que decir al respecto. Así pues, Losavio *et al*. (2018) exploran el impacto del Internet de las Cosas en temas como la privacidad y autonomía personal, la toma de decisiones políticas y su elaboración, y los procesos jurídico-legales; haciendo que todo este entramado sea beneficioso para los encargados de desempeñar estas funciones, pero también para aquellos que buscan sacar provecho de las mismas desde la ilegalidad. De esta forma, se demuestra que el tema de la Seguridad Digital es un tema multidisciplinar, y la importancia de que sea abordado desde los diversos sectores dentro de la academia.

Anteriormente, en el presente documento se trató el tema acerca de la Infraestructura Informática Crítica, y en este instante cobra importancia resaltar las líneas de investigación que desde la academia han avanzado sobre este tema. Al igual que el Internet de las Cosas, se encuentra la convergencia de varios campos del conocimiento alrededor de este tema, y por supuesto desde la ingeniería ya existen varias propuestas, ejemplo el documento elaborado por García Font *et al*. (2014) que estudia el vínculo entre las plataformas *Smart City* y la Infraestructura Crítica, y los potenciales fallos en cascada que se pueden dar a causa de esta. Como es de esperarse, las ciencias militares también hacen aportes importantes frente al estudio de la Seguridad Digital en la Infraestructura Crítica, así Giudici (2013) establece la importancia entre la Seguridad Digital y la Infraestructura Crítica como teatro de operaciones.

Es más, las ciencias sociales no se ven limitadas en este aspecto de la Seguridad Digital, por el contrario, dentro de sus

distintas disciplinas se pueden encontrar aportes interesantes que proveen de otras perspectivas. Por ejemplo, desde la economía se estudia la dependencia de la Infraestructura Crítica hacia las nuevas tecnologías digitales, y cómo esta puede afectar la adecuada administración de los recursos (Kepchar, 2016). La antropología también se ha manifestado al respecto, ideando aprovechar estas infraestructuras digitales para el avance del desarrollo académico en las sociedades (Kenner, 2014).

En cuanto a la ciberinteligencia, se pueden determinar dos corrientes importantes abordadas desde la academia: las responsabilidades de las entidades estatales encargadas de este tema, y la importancia de la *deep web* o red profunda, y en especial dentro de esta, la *dark web* o red oscura en este tipo de actividades. En primer lugar, Eom (2014) hace una propuesta desde una perspectiva operacional, en donde los roles deben ser asignados según las fases de una operación, y al tratarse de este nivel estratégico, se coordina lo táctico, lo estratégico y las políticas públicas alrededor de las acciones. Por su parte, Martín (2016) establece la ciberinteligencia como una responsabilidad de las instituciones tanto públicas como privadas, y hace un llamado para hacer el paso definitivo de una posición reactiva en el ciberespacio, a una proactiva.

En segundo lugar, y del mismo modo, también Martín (2017) hace referencia a la vasta cantidad de información existente dentro de la *deep web* y la *dark web* referente a amenazas, vulnerabilidades y riesgos, recordando que la materia prima de la Inteligencia es precisamente la información. Asimismo, también se encuentran documentos que no solo definen de manera precisa lo que es la *dark web*, sino que además hacen una clasificación y taxonomía de las herramientas de tecnología y herramientas de acceso y monitoreo a este sector del ciberespacio, de modo que puedan ser aprovechadas para avanzar en temas de Inteligencia, y encontrar los vacíos de investigación en este campo (Fachkha & Debbabi, 2016). Como se puede evidenciar, dentro de la cibe-

rinteligencia la academia tiene un amplio campo de acción por recorrer, dando una luz promisoria a las investigaciones que se adelanten sobre este tema.

Otro campo de estudio importante, y que a veces puede ser subestimado, es el tema de la ética en el ciberespacio, que por su naturaleza particular es claramente un tema interdisciplinar, siendo la ética un tema de amplio rango y cuyo estudio parte de la misma filosofía. Ejemplo de esto, son las obras que buscan dilucidar a quién debe atribuírsele la responsabilidad por fallas cibernéticas que pueden acarrear situaciones lesivas a usuarios y/o sistemas, como lo plantea Dennett (2014) con su elocuente título *"When HAL kills, who's to blame?: computer ethics"*. Ya más puntualmente, un sector importante para la ética ciberespacial es la administración pública, como lo señala Kernaghan (2014) con los cambios éticos que traen las TIC para los servidores públicos en el cumplimiento de sus labores, o cómo la ética es una consideración importante en las plataformas de *Smart City* e Internet de las cosas (Losavio et al., 2018).

Desde otra perspectiva, la ética cibernética también tiene aportes importantes para su propia fuente de producción, es decir, cuáles deben ser las aproximaciones éticas de la academia en esta era de expansión digital, y en especial en sus actividades específicas. Es así, que por un lado, se encuentran textos que plantean los nuevos retos éticos a los que se enfrentan los educadores en su labor, gracias a la aparición del Internet y las TIC y su importante influencia en el sector educativo (Olcott *et al*., 2015). Por otro lado, también es de especial atención los cuestionamientos éticos que trae consigo la investigación, aún más si se consideran nuevos procedimientos como el *big data*, al poderse infringir el derecho a la privacidad de las personas, tomando datos que en principio son personales pero se encuentran en el ciberespacio, sumado al hecho de que la investigación académica es de tipo público (Sula, 2016).

De este modo, se han cubierto los aspectos realzados en la mesa de trabajo mencionada como los más importantes a cubrir e investigar por parte de la academia colombiana, pero esto no significa que sean los únicos relevantes. Por ejemplo, una vez más las ciencias sociales señalan los importantes cambios que trae la Seguridad Digital, como se observa desde la sociología política y los retos que afronta la gobernabilidad de las sociedades gracias a la aparición del ciberespacio (Eijkman, 2014); en efecto, hoy en día que el concepto de Seguridad abarca mucho más que la Defensa del Estado, este tipo de avances académicos son una contribución importante. Por ese motivo, es que autores como Sancho (2017) que evidencian las facilidades para la gobernabilidad que provee el ciberespacio, pero también los riesgos que se enfrentan dentro del mismo, máxime de su capacidad de llegar hasta toda, o casi toda, la ciudadanía.

Otro aspecto importante para tener en cuenta desde la academia es lo pertinente con el derecho del ciberespacio, o cómo las situaciones generadas por este deben ser reglamentadas o reguladas, ya que han sido ampliamente referenciados los retos legales desde el advenimiento del Internet frente a temas tales como derechos de autor, pornografía, datos personales, etc. En consecuencia, se encuentran libros completos que cubren todos estos distintos aspectos legales y los nuevos retos que se les presentan desde el ciberespacio, como el que lleva la autoría de Kosseff (2017), que cubre un amplio rango de temas, desde protección de datos, litigios, y sociedades público-privadas; pasando por *hacking*, monitoreo, Ciberseguridad y otros temas propios del ciberespacio; hasta llegar a temas de gobierno y Derecho Internacional. Este último aspecto, el Derecho Internacional, es de vital importancia puesto que al trascender fronteras, el ciberespacio logra imponer nuevos desafíos a las relaciones entre Estados y demás actores internacionales (Segura, 2017).

Llegado a este punto, se ha podido revisar cuáles son los principales temas a abordar en el presente por parte de la acade-

mia respecto a Seguridad Digital, y se ha podido constatar que todavía existe un amplio campo por investigar. De modo que siguiendo las propuestas hechas por los mismos académicos, se ha podido verificar la importancia de revisar desde este sector temas como Internet de las Cosas, Infraestructura Informática Crítica, Ciberinteligencia y Ética digital, además de notar otros temas dignos de mención dentro de la Seguridad Digital como la gobernabilidad digital y el derecho en ciberespacio. Solo en estos temas, el interesado en llevar a cabo una investigación académica en uno de ellos encontrará mucha tela por cortar.

A pesar de esto, no se puede asegurar que el campo de acción de la academia esté limitado a estos temas, o que la anterior haya sido una lista totalmente omnicomprensiva, y todavía quedan temas por revisar más adelante. Así entonces, en el siguiente apartado se hará una revisión de los retos futuros de la academia en materia de Seguridad Digital, si bien no siempre puede haber plena certeza de lo que depara el futuro, es posible mirar las tendencias que se han venido generando y en sus posibles consecuencias. Precisamente, es esto lo que se revisará a continuación.

4. CIBERSEGURIDAD Y ACADÉMICA HACIA EL FUTURO

Una vez revisados los alcances y las funciones del sector académico en cuanto a Ciberseguridad, queda preguntarse cuál va a ser la proyección a futuro en este campo, y qué novedades vendrán consigo. Lo interesante de esta mirada prospectiva es que, al darse los avances en ciberespacio de una manera rápida y vertiginosa, los ítems aludidos en la sección anterior bien podrían considerarse como el futuro del ciberespacio, a la vez que su presente, y muy posiblemente al leerse estas líneas, su pasado. Por ello mismo, se hace necesario reconocer a tiempo las nuevas tendencias que se proyectan y presentan en lapsos de tiempos futuros.

Para lograr tal cometido, se tomará como referencia el documento elaborado por la empresa ESET (2018), debido a su pertinencia y actualidad, frente a otros documentos elaborados por empresas de Seguridad Digital cuyas proyecciones se hicieron en años anteriores. Así, siguiendo esta directriz, los temas considerados de relevancia futura son a saber: *ransomware*, ataques a Infraestructura Crítica, investigación policial de *malware*, *hackeos* a la democracia, y datos personales (ESET, 2018). Así pues, en este aparte se revisarán los aportes de la academia a los ítems referenciados, como también a aquellos que puedan surgir de la revisión de estos.

En el primer caso, el *ransomware* es definido como el *software* malicioso que niega el acceso a unos datos o información hasta que se pague un rescate (Alessandrini, 2016), de ahí su nombre. Por su parte, investigando sobre los avances académicos más recientes hechos al respecto, es curioso notar los contrastes entre lo escrito por la academia hispanoparlante y lo elaborado por la academia angloparlante, dado que los primeros todavía se concentran en casos bastantes específicos como lo fue el caso Wanna Cry (Martínez & Hernández, 2017). O por de forma un poco más general, se estudia el comportamiento del *ransomware* en dispositivos más específicos, como por ejemplo los dispositivos Android (Sánchez, 2018).

Así mismo, en el caso angloparlante, lo que se estudia respecto al *ransomware* va más orientado hacia temas de prevención tanto a nivel técnico como social, como lo es la detección temprana de este tipo de *software* malicioso usando características de tráfico HTTP (Cabaj *et al*., 2018). En cuanto al aspecto social, se encuentran trabajos que abordan la prevención ante este tipo de amenazas en la detección de posible ingeniería social tan común en estos casos (Thomas, 2018), en particular, en los casos de empleados públicos o de empresas privadas, que es donde son más frecuentes este tipo de ataques. Por lo tanto, es claro que las necesidades y vulnerabilidades frente al tema del

ransomware varían dependiendo de la ubicación geográfica, y más puntualmente, el nivel de dependencia que se tiene del ciberespacio, o su precariedad.

En ese sentido, trayendo nuevamente a colación el tema de la Infraestructura Crítica, pero ahora concentrándose en el tema de ciberataques hacia esta, es claro cómo este campo muestra ese vínculo entre presente y futuro mencionado al inicio de este aparte. Por supuesto, ya se encuentran en el mercado libros especializados sobre la protección de la Infraestructura Crítica de ataques provenientes del ciberespacio, y su abordaje es omnicomprensivo yendo desde las macroestructuras hasta los aparatos personales, que es el ejemplo del *Handbook on Securing Cyber-Physical Critical Infrastructure (Das et al., 2012)*. De igual manera, se encuentran documentos que idean mecanismos de valoración de ataques cibernéticos a infraestructuras críticas (Genge *et al*., 2015), o bien que se delimitan a la protección de elementos específicos de la Infraestructura Crítica, como lo son los recursos energéticos (Correa-Henao y Yusta-Loyo, 2013).

Es de destacar, el hecho que en la región suramericana se adelanten trabajos que buscan la protección de la Infraestructura Crítica de sus respectivos Estados, lo cual puede ocupar los vacíos evidenciados en la primera sección de este capítulo. Como es de esperarse, Brasil hace un interesante aporte desde la academia a la Seguridad Digital de su infraestructura, presentándola como un imperativo de su gran estrategia, y como soporte de sus metas como potencia regional (Amaral, 2014). Pero si se trata de llenar vacíos temáticos, es interesante el planteamiento que hacen Robert Vargas *et al*. (2017) al proyectar una visión político-estratégica de la Seguridad Digital de la Infraestructura Crítica ecuatoriana, resolviendo así el aporte de la academia de su país a ese tema.

A otro nivel, tomando en consideración la Seguridad Digital de la ciudadanía se torna evidente la necesidad de vincular

los procesos policivos y jurídicos con la investigación sobre *malware*, donde se encuentran nuevamente puntos de intersección entre la ingeniería y las humanidades, específicamente los estudios en derecho. Por un lado, desde el derecho, se tienen las investigaciones hechas respecto a los procesos que deben llevarse a cabo para la investigación y enjuiciamiento por la producción de este tipo de *software*, lo cual a hoy en día sigue siendo difícil de rastrear y legislar (Rayón y Gómez, 2014). Por otro lado, desde la ingeniería, se hacen estudios prospectivos sobre el futuro del *malware*, como es el caso del artículo elaborado por Pathak & Nanded (2016), donde se perfila el *ransomware* como tendencia criminal a seguir, confirmando lo escrito en párrafos anteriores.

A pesar de las tendencias referidas en el párrafo anterior, la tendencia más marcada encontrada en esta investigación es el tema de la informática forense, que también contiene así aporte de los campos académicos mencionados. Así, por el lado del derecho se contemplan los dilemas técnicos, legales y éticos que se presentan al llevar a cabo esta actividad, en espacial, en un tema de actualidad y futuro en temas ciberespaciales, como lo es la nube informática, cuyas características virtuales hacen estas delimitaciones más difusas (Broucek & Turner, 2013). En cuanto a la ingeniería, lo que se explora dentro de este campo académico es precisamente cómo las nuevas tecnologías pueden mejorar o entorpecer estos procesos forenses, y los impactos que pueden tener en cuanto a la investigación policial (Piccirilli, 2016).

Ahora bien, cambiando de tema, y considerando cuándo lo ciudadano impacta lo político, demostrando en cierta medida cómo el ciberespacio debe entenderse desde el nivel operacional, los *hackeos* a la democracia son una de las amenazas presentes que dominan la agenda. Una buena muestra de esto, es el artículo desarrollado por el trabajo conjunto realizado por varios profesores doctorales de las ciencias sociales prove-

nientes de academias prestigiosas, tales como la Harvard Kennedy School o la King's College, haciendo cuestionamientos importantes a raíz de los recientes ataques digitales al proceso electoral estadounidense, poniendo sobre la mesa si este tipo de procesos deben ser considerados parte de la Infraestructura Crítica (Shackelford *et al*., 2017). Así, resaltando lo dicho, se encuentra el trabajo de Torres-Soriano (2017) "Hackeando la democracia: operaciones de influencia en el ciberespacio", en donde se valoran los impactos electorales desde las acciones en el ciberespacio.

Pero el análisis del *hackeo* a la democracia no se limita a las amenazas externas, sino que también se evalúa cómo el mismo proceso desde su interior puede ser sujeto a explotaciones por parte de *hackers* o a fallas masivas (Yasunaga, 2017). Del mismo modo, también se deben considerar aquellos procesos distintos a las votaciones que son igualmente importantes para un sistema político democrático; se toma por caso la reflexión hecha por Benítez (2013) acerca de la promoción de la democracia en el ciberespacio, vista a través del lente de la movilización social, y qué tantas garantías hay de que esta se dé. Como puede evidenciarse, la relación entre Seguridad Digital y democracia es todo un campo de análisis el cual debe ser abordado por la academia, y que marca pauta para investigaciones futuras en las múltiples aristas que este tiene.

Un ítem que claramente refleja esa interacción entre pasado, presente y futuro de la Seguridad Digital, es el tema de la protección de datos personales, demostrando ser un tema recurrente que en cada momento presenta nuevos retos. Así, siguiendo esta línea, el problema ya no se centra exclusivamente en el acceso de estos grandes datos o *big data* disponibles en el ciberespacio, ahora está también el dilema de cuál debe ser el uso adecuado de estos datos, ya que este uso contempla varios riesgos para las empresas y el tercer sector (Tascón, 2013). Asimismo, una prueba fractal de las interconexiones generadas

por este, el quinto campo estratégico, son los estudios llevados a cabo sobre los grandes datos recolectados a través del Internet de las cosas, el cual se revisó en este texto en el aparte anterior, el cual ya cuenta con sus propios estados de la cuestión (Chen *et al*., 2015).

Aun con estos avances y nuevos alcances de los estudios alrededor de los datos personales, dichos estudios no se limitan exclusivamente a su protección y uso, nuevos retos aparecen que se pueden vincular a otros temas anteriormente revisados como la ciberinteligencia. Uno de estos nuevos retos, consiste en que además de la protección y uso de grandes datos y datos personales existe también el riesgo de que estos sean falsos, y la ausencia de veracidad de estos datos puede conducir a lecturas erradas sumando a confusiones y estimaciones equivocadas (Lu *et al.*, 2014). Fuera de esto, es de primordial interés un libro desde el derecho como el redactado por Garriga (2016), cuyos señalamientos hacia el *big data* van desde la dignidad ciudadana y el derecho a la intimidad, hasta la protección de datos dentro y fuera de las fronteras.

En suma, en este aparte se ha podido revisar cómo algunas tendencias en Seguridad Digital no solo se han mantenido desde el auge del ciberespacio, sino que se mantienen en el presente, e incluso proyectan nuevos retos en el futuro previsible. Tal es el caso de temas ya antes abordados en este capítulo, como es el caso de la protección digital de la Infraestructura Crítica, el *malware*, y la protección de datos personales; a medida que avanza la tecnología digital, estos ítems toman nuevas facetas, y el sector académico no puede quedar rezagado ante estas, como acá se ha probado. Similarmente, aparecen nuevas tendencias que pueden tener una semilla en el pasado, pero en el presente y a futuro han cobrado vida propia, como lo son el *ransomware* y los *hackeos* a la democracia, que ya no pueden considerarse parte del conjunto general de *malware* o *hackeo*, ya que sus características les

han otorgado una naturaleza particular que debe ser estudiada con sumo cuidado.

Con estas consideraciones, ya se puede vislumbrar el papel del sector académico frente a la Seguridad Digital, y los importantes aportes que puede dar al Estado, la economía, y principalmente, a la sociedad en general. Quizás, queden ítems y temas por considerar, o puedan aparecer nuevos campos por estimar de los que aún no nos hayamos percatado, esto entendiendo que las miradas a futuro, incluso las más precisas, son especulativas; no obstante, esta primera mirada proveerá los caminos para futuras investigaciones, y como se ha visto, la interconectividad es tal que se pueden vislumbrar los futuros retos con esta exploración. Así entonces, con todo esto en mente, se procederá a revisar los principales hallazgos hechos en este estado de la cuestión, para poder dar pie a las mencionadas investigaciones.

5. CONCLUSIONES Y HALLAZGOS

A lo largo de este capítulo, se ha revisado los alcances del sector académico frente al tema de la Seguridad Digital, tanto el papel que debe desempeñar como parte de la Infraestructura Crítica del Estado, como su importante función social dentro de este. En los documentos revisados, se observaron las distintas tendencias actuales y futuras de los retos que enfrenta la academia frente al tema de Seguridad Digital, sumado a su participación en las políticas públicas elaboradas con el fin de abordar este tema. Por ello, a continuación se presentarán los principales aportes hechos en esta revisión documental, como también algunas observaciones frente a ellos para el fomento de nuevas ideas.

A grandes rasgos, la primera conclusión que se puede extraer es el hecho de que la principal función del sector académico, en cuanto a políticas públicas de Seguridad Digital, es cumplir la

función de formador y capacitador en este tema, lo que queda aún por verse es el alcance de dicha capacitación. La segunda gran conclusión que se puede extraer es la importancia que posee la Infraestructura Crítica para la Seguridad Digital, y cómo este es un aspecto muy a tener en cuenta en cualquier investigación académica sobre este campo, al tener múltiples alcances, riesgo y amenazas. Finalmente, la tercera gran conclusión es la existencia a gran escala de los varios cambios sociales y jurídicos que trae el ciberespacio, y puntualmente, la Seguridad Digital, que deben ser contemplados en este tipo de investigaciones.

Mientras tanto, como se mencionó anteriormente, es bastante claro que el papel principal del sector académico en materia de Seguridad Digital es el de formador y capacitador, lo que no es tan claro revisando las políticas públicas es su alcance. De entrada, no es del todo claro desde que nivel se debe comenzar con esta instrucción, algunas de las políticas públicas revisadas como la israelita o la surcoreana proponen un inicio temprano en este tipo de formación, iniciando desde la misma primaria como semillero o como protección a menores, y otras proponen su implementación desde la Educación Superior. Sumado a esto, en muchas de estas políticas no se establecen delineamientos claros de la instrucción a impartir, y los objetivos específicos o metas claras a lograr con ella.

Una vez establecidas estas metas, también haría falta por aclarar, dada la naturaleza del ciberespacio que difumina los límites entre lo público y lo privado, que tanta incidencia debe tener el uno o el otro en las capacitaciones del sector académico. Aquí, cobra relevancia lo explicado por Roth (2002) en los modelos mixtos de políticas públicas, ya que las políticas públicas de Seguridad Digital abordan un tema de alto interés público, como lo es la Infraestructura Crítica del Estado, pero el sector académico se encuentra conformado por varias instituciones privadas que a su vez cumplen una función social; por lo cual, cabe proyectar la idea de que “las políticas públicas

ya no se conciben como el resultado de una competición entre grupos … sino como el fruto de la negociación entre el Estado y los representantes de los grupos sectoriales involucrados" (p. 33). Ejemplo de esto, fueron las políticas revisadas de Estonia y Estados Unidos, que dan margen de independencia a las instituciones privadas sin que olviden su función ante la sociedad.

En adición a esto, otra consideración que salió a flote en esta revisión documental es el contenido mismo de dicha formación y capacitación, del cual se partió para hacer la posterior revisión en los dos siguientes apartes. Por un lado, aunque pueda parecer obvio se encuentra la capacitación en Seguridad Digital desde el enfoque técnico y de la ingeniería, y muchas de las políticas públicas revisadas apuntan hacia este aspecto, justificado por la renovación constante de las amenazas que provienen del ciberespacio, que aprovechan el mayor número de interconexiones que se dan cada día. Por otro lado, algunas de estas políticas hacían también énfasis en la parte social y humanística de la Seguridad Digital, al tratar la necesidad de un entramado legal para poder llevar a cabo las acciones necesarias, como también la necesidad de llevar a cabo programas de ética digital y buenas prácticas en el ciberespacio.

En virtud de lo anterior, retomando entonces el segundo eje del presente estado de la cuestión, en cómo ejecuta sus acciones el sector académico en cuanto a capacitación sobre Seguridad Digital, se recuperaron algunos trabajos ya existentes sobre dicho procedimiento, como también las principales tendencias que deben guiar las investigaciones al respecto. De esta manera, se visibilizó el trabajo en curso que lleva a cabo la Escuela Superior de Guerra "General Rafael Reyes Prieto", en cuanto a Ciberespacio y Seguridad Digital, no solo por el hecho de poseer ya en su bibliografía publicaciones al respecto, sino también por el trabajo en curso que se está efectuando en la materia, y del cual este capítulo hace parte. Así mismo, se revisaron proyectos que se aproximan a casos puntuales y buscan aportar nuevas

visiones y soluciones a los problemas inherentes a la Seguridad Digital, o aquellos que buscan integrar a las partes interesadas en este tema para poder adelantar acciones conjuntas de mayor impacto y alcance.

Agregado a esto, la interconectividad del ciberespacio se pudo reflejar en los temas propuestos en la mesa de trabajo, al no tratarse del todo de ítems separados entre sí, sino que se traslapan el uno al otro en temas de Seguridad Digital. Por ejemplo, el tema del Internet de las Cosas hace que haya nuevas conexiones y una mayor multiplicidad de efectos de cascada, los cuales pueden afectar la Infraestructura Informática Crítica cuya prioridad ha sido transversal al estudio realizado en estas páginas, ya que de su protección depende el normal funcionamiento del Estado. Análogamente, desde la ciberinteligencia se deben estudiar los alcances de la *deep web*, y más que todo de la *dark web*, para encontrar los patrones y trazas de posibles amenazas hacia la Infraestructura Crítica y la ciudadanía, pero esto no nos debe alejar de la ética y buenas prácticas, que también se han recalcado como tema transversal.

No obstante, los temas propuestos por la mesa de trabajo no son los únicos relevantes para el sector académico en su papel dentro de la Seguridad Digital, en este trabajo también se arriesgaron otras propuestas que se salen un poco del esquema mental que se tiene al hablar de este tema. En este punto, se debe contemplar el concepto de Seguridad más allá de su acepción tradicional como la protección ante unas amenazas físicas, sino también como la manutención de la estabilidad a futuro (Buzan & Hansen, 2009); de ahí, la importancia del derecho tanto nacional como internacional, como el aporte que puedan brindar ciencias sociales como la ciencia política, para la manutención de la gobernabilidad digital y los impactos sociales provenientes del ciberespacio. Todo esto, simplemente demuestra cómo este, el tema de la Seguridad Digital, es interdisciplinar y transdisciplinar, y qué mejor sector para abordar un tema así que la academia.

De manera que, sabiendo esto, ya es posible echar una mirada hacia el futuro en el papel del sector académico y la Seguridad Digital, lo cual fue la temática del tercer aparte de este capítulo, y como se observó, es un tema que abarca simultáneamente pasado, presente y futuro. Nuevamente, se hallaron temas que en principio parecen ser temas aparte con solo la Seguridad Digital como eje común, pero que nuevamente se puede notar una interconexión y una interdependencia entre ellos, evidenciada dentro del aparte con la interacción Estado-Infraestructura Crítica-sociedad. Así, subrayando una vez más, la importancia de la interdisciplinaridad que el sector académico puede aportar para estos casos, y así poder integrar distintas disciplinas y distintos niveles.

En efecto, el estudio de *ransomware*, ataques a Infraestructura Crítica, investigación policial de *malware*, *hackeos* a la democracia, y datos personales, marca la pauta a seguir para el sector académico en investigaciones presentes y futuras. En este instante, fue posible vislumbrar cómo la Infraestructura Crítica no es un concepto estático, donde ya se propone que los procesos democráticos hacen parte de esta, debido a la importancia que en ellos recae, y las vulnerabilidades que estos tienen de cara al ciberespacio, las cuales han empezado a salir a la luz pública. De igual manera, en el caso suramericano se puede observar cómo la protección de la Infraestructura Crítica es una herramienta de vital importancia para la proyección regional e internacional.

En cuanto a los otros dos ítems, estos también demostraron tener interconectividad entre sí y los dos anteriores, además de hacer la meta-referencia propia de este caso en donde también se interconectan disciplinas y sectores sociales. Tanto en el estudio y detección del *ransomware*, el *software* malicioso que secuestra información a cambio de un rescate, como en la colaboración entre Policía y empresa privada en la investigación de *malware*, se denota la amplitud de estos campos, y cómo se

requiere de la colaboración de las varias partes interesadas para llegar a un resultado exitoso. De nuevo, se tiene ante sí la necesidad de una visión integradora para enfrentar los nuevos retos, que solo el sector académico puede proveer.

Con todo y todo, es claro que hay mucho por recorrer en materia de Seguridad Digital, y el sector académico en su papel de capacitador y formador no puede quedarse por fuera de cualquier política pública al respecto. Esto solo es posible si se tiene en cuenta que el ciberespacio va más allá de una simple red de computadores y aparatos interconectados, y se miden los impactos de los usuarios detrás de ellos, que son precisamente los que aprovechan este nivel estratégico, ya sea en beneficio de la sociedad y el Estado, o en su detrimento.

En este capítulo, se proveyeron los primeros lineamientos para futuras investigaciones y nuevos desarrollos en materia de Seguridad Digital, buscando así una mejora de las condiciones de Colombia y su ciberespacio. Por ello, se resaltó aquí la importancia del sector académico como faro que debe guiar los procesos que se lleven a cabo a todo nivel, vinculando lo estratégico del Estado, con lo particular de lo ciudadano y lo empresarial. Es así, que la academia es la luz que guía a la Seguridad Digital en el caos virtual.

CAPÍTULO IV

ESTADO DEL ARTE DE LA GESTIÓN DE RIESGOS EN SEGURIDAD DIGITAL EN EL SECTOR GOBIERNO EN EUROPA Y AMÉRICA DEL NORTE[15]

Rafael Vicente Páez Méndez [16]
Escuela superior de Guerra

1. INTRODUCCIÓN

La Gestión de Riesgos en el entorno digital es un tema de vital importancia para todos los gobiernos del mundo, por tal razón es necesario generar políticas públicas que permitan proteger el entorno cibernético del país utilizando un modelo de Gestión del Riesgo basado en el contexto, de manera que se pueda identificar el riesgo, valorarlo y minimizarlo hasta niveles aceptables después de aplicar los controles correspondientes.

La Estrategia de Gestión de Riesgos es un proceso dinámico, ya que es necesario adaptarse a los cambios de la sociedad en ámbitos políticos, sociales, económicos, entre otros, por lo tanto,

15 Capítulo de libro resultado del proyecto de investigación titulado "Gestión de Riesgos en Seguridad Digital" de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra, que a su vez hace parte de la línea de investigación 'Seguridad digital' del grupo de investigación 'Masa Crítica', reconocido y categorizado en (C) por Colciencias. Registrado con el código COL0123247, está adscrito a la Escuela Superior de Guerra de la República de Colombia.

16 Docente (Universidad Pompeu Fabra, Barcelona-España), actualmente, Profesor asociado (Pontificia Universidad Javeriana, Bogotá), miembro del Grupo de Investigación SiDRe. Doctor en Ingeniería Telemática con énfasis en Seguridad; Ingeniero de Sistemas con especialidad en Seguridad Informática. Investigador de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto". Patrocinado por el Patrocinado por el Ministerio de Tecnologías de la información y las comunicaciones.

es necesario generar modelos que permitan realizar una gestión precisa y efectiva en el contexto de la realidad de cada país, sin embargo, existen iniciativas que pueden ser adaptadas a diferentes necesidades para generar y adoptar un modelo propio.

Tanto la industria como los gobiernos están permanentemente desarrollando estrategias de Gestión de Riesgos y alineándose con buenas prácticas y estándares internacionales como ISO/IEC 27001 y 27002. Por otra parte, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) afirma que la Gestión de Riesgos ayuda a proteger y soportar las actividades sociales y económicas y provee un marco general de 8 principios de alto nivel en Gestión de Riesgos en Seguridad Digital con el fin de orientar a las organizaciones tanto públicas como privadas en el desarrollo de un modelo propio de Gestión de Riesgos (Organisation For Economic Co-Operation And Development, 2015).

2. SITUACIÓN ACTUAL

En Europa, se conformó la Agencia Europea de Seguridad de las Redes y de la Información (*EuropeanUnion Agency for Network and Information Security* – ENISA)[17] en donde se publican diferentes documentos sobre Seguridad y particularmente, en materia de Riesgos los clasifica en una escala temporal en *Riesgos actuales*, *Riesgos emergentes* y *Riesgos futuros*; de esta manera, se proveen las herramientas, los métodos y las buenas prácticas, para que entidades tanto gubernamentales como privadas las utilicen como guía con el fin de enfrentar las amenazas.

- En **Albania**, las bases de datos del Gobierno y el uso público de la información se encuentran en una etapa temprana de desarrollo y aún se considera como una expectativa potencial

17 https://www.enisa.europa.eu/topics/threat-risk-management/risk-management

futura para una mejor gobernanza, se contemplan avances en la implementación del gobierno electrónico en términos de intercambio de información entre el público servidores, ciudadanos, agentes sociales y económicos. Así mismo, Transparencia en la gobernanza con relación a los ciudadanos y los medios y Descentralización y fortalecimiento de la autonomía local; también como participación de los ciudadanos en la gobernanza local, hoy es un desafío a pagar. Los programas políticos de los gobiernos no han considerado una prioridad la información de sistemas de gestión en Albania, especialmente todavía en la administración pública. Así, contemplando consideraciones secundarias, los sistemas de información a nivel local y central aún no son integrado e incompleto, este es un proceso extenso que atraviesa etapas como la difusión electrónica de información a través de la presencia en la *web* hasta la transformación total del gobierno a través del proceso de ofrecer servicios públicos confiables, seguros y de fácil acceso en línea con una participación activa de los ciudadanos y negocios. La Gestión de Riesgos en Seguridad Digital se tiene en cuenta para lo que el Gobierno albanés llama la "Iniciativa de Desarrollo", anunciada en abril de 2002 en la Conferencia Internacional "E-goverment para el Desarrollo" en Palermo, que promovió la puesta en marcha y la implementación de proyectos de Gobierno electrónico en las naciones beneficiarias, incluida Albania. El proyecto se lanzó a principios de 2005, se centra en la asistencia técnica para establecer un sistema de correo electrónico gubernamental, una intranet y el despliegue de los sistemas y bases de datos existentes en el Gobierno.

- En **Alemania**, la Oficina Federal Alemana para la Seguridad de la Información es la autoridad nacional de Ciberseguridad y es la encargada de determinar la Gestión de Riesgos en Seguridad Digital, haciendo control de la Seguridad de la información en la digitalización a través de la prevención, detección y reacción para el gobierno, las empresas y la sociedad. Esta entidad se encarga de promover la seguridad de TI en Alemania por medio de tres divisiones: el CERT-Bund (Equipo de Respuestas de

Emergencias Computacionales), el IT *Situation Centre* (Monitoreo y alertas tempranas), el IT *Crisis Reaction Centre* (Manejo de Crisis Nacionales) y el *Cyber Response Centre* (Cooperación con otras entidades federales para la Seguridad) (Bundesamt für sicherheit in der informationstechnik, 2009). Al evidenciar que en la última década el proceso de digitalización de la información avanza a grandes pasos y de igual forma impulsan la comunicación, comercio y entretenimiento se ha adoptado el término "gobierno electrónico" al comprobar la necesidad de seguridad de TI, ya que las amenazas pueden llegar a pasar desapercibidas a primera vista. La Ciberseguridad se está convirtiendo en una de las áreas de más rápido crecimiento en la política mundial. Es imposible para un Estado gestionar el escape de la ola emergente de ciberataques. Los efectos generalizados de las armas cibernéticas han socavado los sistemas existentes de detección e interceptación de los Estados. Las autoridades de Alemania reafirmaron la importancia de la Ciberseguridad y su relevancia para el futuro del país. El Ministerio de Seguridad Nacional de Alemania cree que las amenazas a la Seguridad cibernética prevalecen en este país debido a la digitalización de la sociedad y al desarrollo de infraestructura estatal.

- En **Andorra**, se ha estado a la vanguardia de la práctica de Seguridad de la información durante muchos años, creando e implementando programas efectivos para gobernar y administrar los riesgos. Han desarrollado y operado Centros de Operaciones de Seguridad, dirigieron prácticas de respuesta a incidentes de Seguridad, crearon marcos de políticas y gobernanza, y han implementado y operado equipos de investigación digital. El Gobierno de este país cree firmemente en el posicionamiento de la Seguridad de la información como un habilitador de negocios mediante la promoción de un enfoque arquitectónico y basado en el riesgo para el desarrollo y la gestión de programas. Es por esto que creen necesario implementar un control, y eso es para administrar el riesgo, es decir, para comprender completamente el impacto del control; debe poder medir y evaluar el riesgo.

Se pretende también que el uso efectivo de la Gestión de Riesgos en la Seguridad de la información tenga dos grandes beneficios. En primer lugar, permitir a los diferentes actores gubernamentales poder tomar decisiones razonables sobre las inversiones en Seguridad de TI e impulsar la aceptación de nuevos controles, de manera que se pueda clasificar como tratamientos de Gestión de Riesgos. Esto con el fin de ayudar a posicionar la Seguridad de la información como un habilitador de negocios, y no solo como un centro de costos. En segundo lugar, se espera garantizar que las decisiones fundamentales de Gestión de Riesgos no sean retenidas por los líderes empresariales y ponga la responsabilidad del riesgo en el lugar al que pertenece como lo es directamente los ministerios de Defensa, del Interior y de Tecnología de la Información. Lo anterior con el fin de medir el costo, que puede ser financiero, reputacional o reglamentario, a lo largo del tiempo y su impacto en la eficiencia del negocio también puede ser extremadamente desafiante.

- En **Austria,** la política de Ciberseguridad de vanguardia es una cuestión transversal que se tiene en cuenta en muchas esferas de la vida y las políticas de esta nación. Se considera que debe modelarse sobre la base de un enfoque integral e integrado, de modo que se pueda permitir la participación activa y se logre implementar con un espíritu de solidaridad, es por esto que el canciller Sebastian Kurtz actualmente pretende implementar: una Política Integral de Ciberseguridad es decir, que la Seguridad externa e interna, así como los aspectos de Seguridad civil y militar están estrechamente relacionados.

Cabe aparte indicar, que la Ciberseguridad va más allá del alcance de las autoridades de Seguridad tradicionales y comprende instrumentos de muchas otras áreas de políticas. Esta nación considera que una Política Integrada de Seguridad Cibernética debe hacer hincapié en la distribución de tareas entre el Estado, la economía, el mundo académico y la sociedad civil. Así, incluyendo medidas en las siguientes áreas: gestión estratégica, educación

y capacitación, evaluación de riesgos, prevención y preparación, reconocimiento y respuesta, limitación de efectos y restauración, así como desarrollo de capacidades y capacidades gubernamentales y no gubernamentales. Una Política Integrada de Seguridad Cibernética debe basarse en un enfoque cooperativo tanto a nivel nacional como internacional, además debe ser proactiva de modo que se pueda trabajar para prevenir las amenazas al ciberespacio y las personas en el ciberespacio o para mitigar su impacto.

Además, se quiere basar la Gestión de Riesgos en Seguridad Digital en la solidaridad teniendo en cuenta el hecho de que, debido a la naturaleza global del espacio cibernético, la seguridad cibernética de Austria, la UE y toda la comunidad de naciones está muy interconectada. Por lo tanto, se requiere una cooperación intensiva basada en la solidaridad a nivel europeo e internacional para garantizar la Ciberseguridad. Los principios universales de seguridad de las TIC para una **Austria digital** son plenamente aplicables a la Ciberseguridad: confidencialidad, integridad, aplicación obligatoria, autenticidad, disponibilidad, así como privacidad y protección de datos.

- En **Australia**, el Gobierno cuenta con un marco de referencia denominado PSPF (*Protective Security PolicyMarco de referencia*)[18] e incluye la Gestión de Riesgos que está alineadacon el estándar ISO 31000:2009 (Australian/Standards, 2009) y HB 167:2006 *Security RiskManagement* y con las políticas de Gestión de Riesgos de la Mancomunidad de Naciones, de modo que se pueda tener un sector público más productivo, innovador y eficiente, dando así un enfoque a la Gestión del Riesgo para alcanzar los objetivos estratégicos de la Mancomunidad y limitar la burocracia innecesaria. La gestión efectiva de riesgos, basada en el buen juicio y la mejor información disponible, mejora la capacidad de la Commonwealth para identificar, administrar y

18 https://www.protectivesecurity.gov.au/resources/Documents/Protective-Security-Policy-Framework-Map.pdf

obtener los máximos beneficios de los nuevos desafíos y oportunidades. (Commonwealth of Australia, 2014). La Oficina de Gestión de Inversiones Digitales se ha establecido dentro de la Agencia de Transformación Digital (ATD) del Gobierno australiano para supervisar todos los proyectos importantes de TIC e inversión digital en todo el Gobierno. Cada año, el Gobierno gasta alrededor de $ 6.2 mil millones en inversiones en TIC. Al desarrollar enfoques nuevos y más estratégicos para el análisis de inversiones, la gobernanza, la Gestión de Riesgos y la gestión de programas y beneficios, podremos proporcionar una mayor transparencia y optimización de la cartera de inversiones del Gobierno. Una prioridad inicial para la oficina será llevar a cabo una revisión de la inversión anual en TIC del Gobierno y proporcionar una imagen completa de los costos, beneficios, riesgos y el estado de todos los proyectos y programas por valor de más de $ 10 millones de dólares. La oficina también se enfoca en establecer alianzas estratégicas continuas en todo el Gobierno para proporcionar garantías independientes y una mejor prestación de beneficios tanto para las agencias como para las personas que utilizan los servicios del gobierno en línea.

- **Azerbaiyán** evidencia cómo, los efectos generalizados de la Tecnología de la Información desarrollaron el sistema internacional como un área fértil para la guerra cibernética. El ciberespacio internacional carece por completo del órgano rector central o de cualquier sistema internacional principal de administración. Sin duda, los Estados están formulando sus alianzas para luchar activamente en el ciberespacio. Pero hasta ahora es difícil separar a los amigos de los enemigos, porque las relaciones de déficit de confianza entre las naciones crearon un sistema ciberespacial anárquico internacional, que en última instancia ha hecho que cada Estado sea vulnerable ante las Fuerzas rivales. Este Estado que se encuentra en la encrucijada de Eurasia, está rodeado por el mar Caspio y la cordillera del Cáucaso, debido a la ocupación armenia de Nagorno-Karabaj y al conflicto armado internacional vino consigo inseguridad cibernética al

mar Caspio y los Estados vecinos antagónicos del Irán clerical y la Rusia nuclear.

Con relación a los ciberataques, Azerbaiyán está tomando varias iniciativas para la protección de su infraestructura digital. El ministro de Comunicación e Informática varias veces destacó la visión del Gobierno en una declaración para el fortalecimiento de la Seguridad de la información de Azerbaiyán. Además, mencionó la ambición de su país de desarrollar una colaboración internacional contra las amenazas prevalecientes de ciberataques organizados. De esta forma, tres importantes instituciones de Gobierno complementan la Defensa de las fronteras cibernéticas de Azerbaiyán: el Ministerio de Comunicación y Tecnología Informacional (MCIT), el Ministerio de Seguridad Nacional (MNS) y la Academia Nacional de Ciencias de Azerbaiyán (ANAS). En resumen, el Gobierno de Azerbaiyán está desarrollando rápidamente su infraestructura de Gestión de Riesgos en Seguridad Digital con la ayuda de ANAS y mejorando la infraestructura digital del Estado. Un entorno digital emergente necesita un sistema de red de comunicación infalible. Sin duda, un enfoque de cooperación multilateral podría aumentar las leyes existentes de Ciberseguridad, pero los esfuerzos individuales activos de los Estados podrían desempeñar un papel más efectivo. Por lo tanto, la combinación de enfoques unilaterales y multilaterales puede contrarrestar mutuamente las abrumadoras amenazas no militares y transnacionales de ciberataques. La base legal de la Ciberseguridad debe fortalecerse en Azerbaiyán porque, las armas cibernéticas en diferentes formas (como el virus *Stuxnet*) ya han intentado destruir la infraestructura cibernética del gobierno (Makili-Aliyev, 2013). Por lo tanto, una red cibernética fuerte y bien asegurada puede prevenir los riesgos de los ciberataques en la infraestructura digital del país. Además, la promoción y avance de las leyes cibernéticas con el establecimiento de un ciberejército se ha convertido en una demanda vital para Azerbaiyán a fin de fortalecer la Ciberseguridad Nacional del Estado. De esta manera, la Seguridad

del ciberespacio es una cuestión de inmensa importancia para Azerbaiyán, porque la creciente dependencia de la industria, el Gobierno y las instituciones financieras de las redes cibernéticas necesita un sistema de información completamente seguro y confiable, que pueda mantener la disuasión cibernética en el mundo ciberespacio.

- **Bélgica** adoptó su Estrategia Nacional de Ciberseguridad en 2013 y en 2014. Estableció el Centro para la Ciberseguridad (CCB) con tres objetivos estratégicos: asegurar un ciberespacio seguro y confiable; proporcionar Seguridad y protección óptimas para las infraestructuras críticas y los sistemas de información gubernamentales y promover el desarrollo de capacidades de Seguridad cibernética a nivel nacional. Toda una sección está dedicada a la Gestión del Riesgo cibernético, que abarca amenazas, vulnerabilidades e impacto (Department, 2014). Desde el lanzamiento del CCB se han tomado medidas para proveer a las autoridades públicas y las empresas con el apoyo y asesoramiento sobre cómo protegerse más eficazmente contra las amenazas cibernéticas. Además, identifica las infraestructuras críticas de Bélgica para garantizar la cooperación entre todos los actores involucrados, es así que en 2017 se lanzó un plan de respuesta de emergencia cibernética, destinado a establecer una forma estructurada para manejar las crisis e incidentes de Ciberseguridad que requieren coordinación a nivel nacional. El objetivo es armonizar las acciones que los servicios gubernamentales toman para gestionar incidentes cibernéticos nacionales y garantizar el rápido, intercambio preciso de información entre servicios (Croo, 2017).

- En **Bosnia y Herzegovina**, los principios básicos para el desarrollo y la aplicación de la Gestión de Riesgos en Seguridad Digital son los siguientes: el principio de voluntad política- una lucha activa contra la delincuencia digital como una de las prioridades de las instituciones en Bosnia y Herzegovina, de la mano de la no discriminación y respeto a las libertades

y derechos de los ciudadanos, de modo que las actividades de la estrategia estén guiadas a garantizar el disfrute de todos los derechos y libertades humanas, de conformidad con la Constitución de Bosnia y Herzegovina, las leyes y las normas jurídicas internacionales. Además, se tienen en cuenta el *Principio de legalidad*, es decir el respeto de la Constitución y las leyes nacionales en esta área, así como ciertas disposiciones de los acuerdos internacionales (instrumentos jurídicos internacionales), de los cuales Bosnia y Herzegovina es signatario de modo que se pueda juzgar de modo eficiente a los ciberterroristas (Ministry of Interior of Republika Srpska, 2017).

Es así que el Gobierno pretende tener una visión única y global en la lucha contra los crímenes cibernéticos, basándose en un enfoque único y global del problema para así tener una correcta coordinación y cooperación de las prácticas y procedimientos para combatir la delincuencia digital tomando como pie un concepto único de sector público y privado, organizaciones internacionales en Bosnia y Herzegovina, la sociedad civil y los ciudadanos. Esto es encaminado de modo que se cuente con profesionalismo y coherencia en todas las áreas de acción en contra de los ciberdelitos de modo que se tiene en cuenta que hace falta una formación profesional continua, educación y capacitación de los servidores públicos, así como el intercambio de experiencias de mejores prácticas y eventos contemporáneos y su cumplimiento de medidas preventivas y represivas. Por otra parte, se espera tener una cooperación internacional activa en los preparativos para unirse a la Unión Europea y garantizar el papel activo de Bosnia y Herzegovina a nivel internacional para así poder garantizar el cumplimiento de los compromisos en la implementación de la Estrategia de Gestión de Riesgos en Seguridad Digital por medio de la supervisión de su implementación con la identificación de las instituciones responsables de la implementación de la misma con compromisos claramente definidos y plazos planificados para monitorear de forma correcta y en consecuencia, se llevará a cabo la evaluación de las medidas correctivas.

- **Croacia** ha identificado algunas debilidades a nivel general en la parte digital como por ejemplo, la baja aceptación de las responsabilidades de Seguridad de los propietarios de datos e infraestructura, una cultura de Gestión de Riesgos desarrollada de manera inadecuada, incoherencia de regulación frecuente a niveles generales y sectoriales, falta de adecuación de los nuevos conceptos de Seguridad, como protección de Infraestructura Crítica, tradición jerárquica de la administración del gobierno, prácticas de intercambio de información muy limitadas (departamentales y sectoriales), falta de educación que apoye el desarrollo de la sociedad virtual y criterios poco claros para la verificación de programas educativos. A raíz de esto la Agencia de Seguridad Nacional croata, desarrolló una serie de recomendaciones e iniciativas enfocadas al sector gubernamental, el programa industrial y la reorganización de iniciativas para compartir información de acuerdo con la Política Nacional de Seguridad para generar una nueva Gestión de Riesgos en Seguridad Digital que involucrara desde la seguridad física hasta el fortalecimiento de la infraestructura informática por medio del refuerzo de sus agencias gubernamentales en esta área. En este país se ven como oportunidades a fututo por medio de dicha Gestión, el desarrollo social en educación y cultura, desarrollo económico en capacidad ciberespacial de interrelacionar los múltiples sectores de la nación brindando una mejor infraestructura y por ende mejores capacidades y productos potenciales.

- En **Dinamarca**, las estrategias digitales del Gobierno conciernen a las autoridades en todos los niveles de este, desde el Estado hasta las regiones y los municipios, es decir, tanto las instituciones administrativas como los ministerios, agencias y las administraciones municipales y regionales, y las instituciones ejecutivas como hospitales, escuelas públicas, universidades, entre otros. La idea de este país es establecer un sector público más simple y más cohesionado en el que se logre proporcionar servicios buenos y eficientes a individuos o empresas, sobre la base del conocimiento que ya se tiene. Para que esto

se convierta en realidad, las autoridades deben en mayor medida poder intercambiar y acceder a datos relevantes sobre individuos de manera segura; no menos importante en situaciones en las que muchas autoridades están involucradas. Por lo tanto, los gobiernos locales, regionales y centrales tienen que trabajar para compartir más los datos siempre que sea posible, relevante y seguro (Danish Ministry of Finance, 2016).

Paralelamente, el uso creciente de datos puede ser respaldado por estándares de datos comunes, formatos de datos estandarizados, arquitecturas de TI comunes y una infraestructura de TI robusta. El mayor intercambio de datos permitirá a las nuevas generaciones de soluciones digitales que puedan encontrar automáticamente los datos necesarios. Las personas y las empresas ahorrarán tiempo porque no tienen que reportar datos innecesariamente. Además, los procesos administrativos y el trabajo de casos se facilitarán si se pueden automatizar los flujos de trabajo manuales y, en algunas situaciones, las decisiones. Un intercambio e intercambio de datos más eficiente entre varios sistemas de TI y unidades organizativas proporcionará a las personas y empresas procedimientos de procesamiento de casos más eficientes y más intervenciones adaptadas y coherentes. En el futuro, las personas y las empresas deberían, en la medida de lo posible, solo enviar la información a las autoridades una vez, en lugar de tener que ingresar la misma información en varios lugares en las soluciones digitales públicas. Un mayor uso y reutilización de los datos también mejorará la base de los servicios públicos prestados. Esto también contribuirá a un sector público más moderno y eficiente y, por lo tanto, liberará recursos que se pueden aplicar a otras prioridades políticas. Estos esfuerzos deben continuar, teniendo en cuenta la legislación sobre el procesamiento de datos personales y el derecho individual a la privacidad.

- En **Estonia**, la agencia encargada de proteger la sociedad digital es la *EstonianInformationSystemAuthority* (RIA) y la Es-

trategia de Ciberseguridad se enfoca en asegurar la provisión de servicios vitales elevando la conciencia del riesgo de Seguridad entre el sector público y los proveedores de servicios críticos y la gestión de riegos. Desde el año 2008 se ha venido utilizando un sistema de tres niveles denominado ISKE[19] el cual asegura un nivel mínimo de Seguridad en el procesamiento de datos en bases de datos estatales y gubernamentales (Vaks, 2017). En el Ministerio de asuntos nacionales y comunicación crearon un sistema llamado "My number" el cual consiste en un número individual de 12 dígitos que le corresponde a cada ciudadano con el fin de facilitar el pago de impuestos, seguros y procedimientos administrativos. El Gobierno estonio se caracteriza por tener unas políticas en la cual le da prioridad a la TIC, lo que hace que dicho actor sea avanzado digitalmente. Así mismo, la difusión del uso de equipos electrónicos en las instituciones educativas y en las instituciones gubernamentales es del 100 %, el uso de la banca virtual para realizar pagos es del 99.8 % siendo este un porcentaje alto. Aparte de realizar transacciones básicas y necesarias para el ciudadano, también ofrecen servicio administrativo en línea de declaración de impuestos, registro de entidades privadas.

La firma Cybernetica inicialmente fue una entidad privada que se consolidó en el año 1997, sin embargo, hoy en día la entidad es conocida como un actor fundamental para proyectos gubernamentales a nivel internacional. La anterior se destaca en el desarrollo de *software* de votos electrónicos, la construcción de un sistema de seguridad en bases de datos gubernamentales por medio del sistema *X-Road*, siendo este sistema una base fundamental para las políticas dirigidas al desarrollo digital. El sistema *X-Road* consiste en una plataforma en la cual protege el intercambio de información entre las entidades participan-

19 System of security measures for information systems (Government of the Republic regulation no. 252 of 20 December 2007; RT I 2007, 71, 440).

tes. Por otra parte, el Gobierno de la mano de la firma Eltes establece como riesgo digital aquellos que se producen debido al desarrollo tecnológico, proveyendo soluciones gracias a la tecnología única y alianzas entre corporaciones y diferentes entidades públicas. Estonia además iniciará una cooperación con Japón con la cual usan la herramienta *VizKey* con el fin de realizar investigaciones delictivas a causa de las transferencias de moneda ilegal y uso de información privilegiada.

- Finlandia, propone una Gestión de Riesgos en Seguridad Digital proyectada para 2020 y promueve en los ciudadanos, las autoridades y las empresas las mejores y más efectivas formas de uso cibernético seguro y el uso de las mejores herramientas en cuestiones de Seguridad cibernética tanto a nivel nacional como internacional buscando ser un precursor mundial en la preparación para la amenaza cibernética y en la gestión de las perturbaciones causadas por estas amenazas. Lo anterior requiere un desarrollo de capacidades en términos de acción y recursos de diferentes entidades de gobierno, las administraciones regionales y locales, así como la comunidad empresarial y las organizaciones, por lo que se estableció un Comité de Seguridad para desempeñar un papel activo en el campo de la Seguridad integral y que actúe como un organismo de cooperación permanente para la planificación de contingencia (Ministry of Transport and Communications, 2016).

- **Francia** plantea una Estrategia en Seguridad Digital con cinco objetivos de Seguridad: *Sistemas de información e Infraestructuras críticas; Datos personales* (Privacidad, confianza digital, etc.), *conciencia* (formación y educación continua); *entorno de las empresas de tecnología digital* (Políticas industriales, exportación e internacionalización) y *el contexto europeo* (Autonomía estratégica digital, estabilidad cibernética). Francia es el objetivo de ataques cibernéticos que dañan sus intereses fundamentales. Hoy, cuando un atacante apunta al Estado, operadores de vital importancia o negocios estratégicos, el objetivo

es la instalación a largo plazo en el sistema de información para robar datos confidenciales (políticos, diplomáticos, militares, tecnológicos, económicos, financieros o comerciales). Razón por la cual desde 2011, las administraciones competentes y los proveedores de servicios han abordado alrededor de un centenar de ataques cibernéticos principales, en la mayoría de los casos con total confidencialidad.

Paralelamente, las posiciones adoptadas por Francia en la escena internacional, sus operaciones militares y ciertos debates públicos son seguidas de ataques cibernéticos destinados a marcar la opinión pública. Por ejemplo, la desfiguración de muchos sitios *web* después de los ataques terroristas contra Francia en el comienzo de 2015 tuvo un impacto técnicamente bajo pero simbólicamente alto deseado por los atacantes. Desde hace varios años, muchos Estados han implementado su voluntad política y medios humanos, técnicos y financieros considerables para llevar a cabo operaciones ciberespaciales en gran escala contra Francia. El Ministerio de Defensa realiza la doble función de garantizar la protección de las redes que sustentan su acción y de colocar la lucha digital en el centro de las operaciones militares. Para consolidar la acción del Ministerio en este campo, se estableció una Unidad de Comando de Ciberdefensa (COMCYBER) que informa al Jefe del Estado Mayor de Defensa a principios de 2017. El Ministerio del Interior tiene la tarea de abordar todas las formas de delito cibernético que afectan a las instituciones y los intereses nacionales, los agentes económicos, las autoridades públicas y las personas. Para ello, moviliza las redes centrales especializadas y las redes regionales de los Directores Generales de la Policía Nacional, la Gendarmería Nacional y la Seguridad Interna. Son responsables de realizar investigaciones para identificar a los perpetradores de ciberataques y llevarlos ante la justicia. Estos servicios contribuyen, entre otras cosas, a los esfuerzos de prevención y a la sensibilización de las personas interesadas (Valls, 2015).

Desde 2010, se han tomado varias medidas para elevar el nivel de Seguridad de los sistemas de información del Estado. Se desarrolló una Política de Seguridad de los Sistemas Estatales de Información (PSSIE), una red de comunicaciones electrónicas interministeriales está en rápido crecimiento y se ha iniciado el despliegue de terminales móviles seguros. Estas medidas, como las destinadas a producir el equipo de Seguridad para proteger la información soberana, movilizan recursos humanos y presupuestarios. Se perseguirán para proporcionar al Gobierno y a sus capacidades militares el nivel de Seguridad adecuado para la preservación a largo plazo de la autonomía de Francia en la toma de decisiones y la adopción de medidas. La aplicación de la Política de Seguridad de los sistemas estatales de información y la eficacia de las medidas adoptadas se evaluarán anualmente. Se transmitirá un informe confidencial anual al Primer Ministro y se informará al Parlamento por medio de indicadores. Con el mismo objetivo de informar al Parlamento, a partir de 2016, los proyectos de ley tendrán una sección en su evaluación de impacto dedicada a la tecnología digital que también incluirá Seguridad cibernética, establecida bajo los auspicios de los funcionarios superiores a cargo de la calidad de la regulación. En términos más generales, los funcionarios superiores a cargo de la calidad de la regulación se asegurarán de que las cuestiones relacionadas con el refuerzo de la seguridad de los sistemas de información se tienen en cuenta en la dirección del proceso normativo.

La prioridad para las autoridades de Seguridad de los sistemas de información competentes debe ser la anticipación y la prevención. Esto implicará garantizar que los productos y servicios digitales o aquellos que involucran tecnología digital, diseñados, desarrollados y producidos en Francia, se encuentren entre los más seguros del mundo. Para lograr este objetivo, las autoridades competentes deberían dirigir sus esfuerzos de comunicación hacia la comunidad científica pública y privada, y los centros de innovación. Cuando los productos y servicios digitales almacenan datos personales o están destinados a los sectores co-

merciales de vital importancia, los servicios estatales proporcionarán los elementos que son útiles para el análisis de riesgos o las recomendaciones requeridas para obtener el nivel de Seguridad que corresponde al uso del producto o el servicio que se diseña o desarrolla. Para los usos que lo justifiquen, también contribuirán a establecer sistemas para evaluar independientemente el nivel de Seguridad y confiabilidad de estos productos y servicios, y para proporcionar a sus usuarios potenciales garantías adaptadas a través del etiquetado. Paralelamente, se debe anticipar el entorno legal para acomodar nuevos productos y servicios. Por ejemplo, la llegada inminente de automóviles autónomos debería incitar al regulador a preparar las condiciones para garantizar la Seguridad de su circulación. La Ciberseguridad debe tenerse en cuenta en los grupos de trabajo internacionales que definen el marco y controlan los procedimientos técnicos. Para otros tipos de productos o servicios, un sistema de identificación adaptado debe informar al consumidor de sus características digitales esenciales y, en particular, del procesamiento de los datos que se recopilan. Para ciertos sectores, como el sector de la salud, se considerará el etiquetado sistemático de productos y servicios digitales.

- En **Grecia** la Ciberseguridad, es decir, la protección de redes, sistemas informáticos y datos del delito cibernético, se ha convertido en una prioridad de Política Nacional como en muchos países que se dan cuenta de su importancia; se están desarrollando nuevas estrategias de Seguridad cibernética para proporcionar protección contra amenazas cibernéticas y salvaguardar la prosperidad económica y social. El objetivo de tales estrategias es mejorar la coordinación gubernamental y definir roles y responsabilidades respecto a la lucha contra la ciberdelincuencia, pero también apoyar la cooperación entre el público y entidades privadas, particularmente Proveedores de Servicios de Internet, y cooperación internacional. Al igual que en otros países europeos, Grecia necesita fortalecer su marco para una protección adecuada. No solo es necesario actualizar el marco legal, sino que también se deben tomar nuevas iniciativas en el

área de la ciencia y la educación con el apoyo gubernamental. Las normas y reglamentaciones suficientes, por un lado, y los organismos gubernamentales específicos para abordar los casos de delitos cibernéticos, por otro lado, indiscutiblemente beneficiarían a la seguridad de la información en Grecia.

- **Holanda** cuenta con una Estrategia de Ciberseguridad (NCSS2) que va por la segunda versión y en la que se incluye la correlación con los derechos humanos, la libertad de Internet, la privacidad, la innovación y los beneficios económicos y sociales. Para lograr los objetivos cuenta con un modelo de 7 capas y en una de ellas está el enfoque basado en riesgos (Centrum, 2013). La principal amenaza para los holandeses está dirigida a las violaciones de la confidencialidad de la información y la incontinuidad de los servicios en línea. Para la comunidad empresarial, la interrupción de los servicios en línea se ha incrementado y a gran escala de la infraestructura digital en los sectores vitales pueden conducir a la interrupción del servicio y, por lo tanto, a efectos sociales indeseables. También existe el riesgo de robo de información competitiva sensible y abuso de datos financieros para fraude. Es por esto que las partes públicas y privadas están iniciando iniciativas, tanto por separado como juntas, para aumentar la resiliencia digital anticipándose a la dependencia cada vez mayor de TI y las amenazas cambiantes. Hasta el momento, muchas organizaciones no tienen medidas básicas en orden, como la administración de parches y actualizaciones o una política de contraseñas. Esta es la razón por la cual las viejas vulnerabilidades y los métodos de ataque aún son efectivos. El usuario final está cargado con una gran responsabilidad de Seguridad, pero la mayoría de las veces tiene poca influencia o incluso conocimiento de las vulnerabilidades que enfrenta en dispositivos y servicios. Por este motivo, el foco sigue siendo aumentar la conciencia de Ciberseguridad de los usuarios.

Para Holanda, es importante mantenerse al día con los rápi-

dos desarrollos y responder a los riesgos que implican. Precisamente por esta razón, pronto se completará una encuesta legal, que apunta a fortalecer la posición del Centro Nacional Holandés de Seguridad Cibernética. Además, el Consejo de Ministros presentará una Estrategia Nacional de Seguridad Cibernética actualizada después del verano que aborda los rápidos desarrollos en el dominio digital. Esta estrategia 2.0 fortalecerá aún más el amplio enfoque de Ciberseguridad con partes públicas y privadas. La Evaluación de Seguridad Cibernética de los Países Bajos está preparada por el Centro Nacional de Ciberseguridad bajo la responsabilidad del Coordinador Nacional de Contraterrorismo y Seguridad. Este documento representa las contribuciones de una amplia gama de actores en la comunidad de las TIC, incluidos los partidos de los sectores público y privado, académicos y ONG.

- **Hungría** se basa en los principios de la Ley Fundamental y en la revisión de los valores e intereses relevantes y en el análisis del entorno de Seguridad del ciberespacio, para definir el objetivo de la Gestión de Riesgos en Seguridad Digital como la determinación de los objetivos nacionales y las direcciones estratégicas, las tareas y el gobierno general. La Gestión de Riesgos en Seguridad Digital apunta a desarrollar un ciberespacio libre y seguro y proteger la soberanía nacional en el contexto nacional e internacional, que ha experimentado un cambio significativo debido al surgimiento del ciberespacio, un nuevo medio que se ha convertido en un factor clave en el siglo XXI. Además, tiene como objetivo proteger las actividades y garantizar la Seguridad de la economía y la sociedad nacionales, adaptar de manera segura las innovaciones tecnológicas para facilitar el crecimiento económico y establecer una cooperación internacional en este sentido en consonancia con los intereses nacionales de Hungría. Esta estrategia indica que Hungría está preparada para asumir responsabilidades en tareas de protección del ciberespacio y tiene la intención de desarrollar el ciberespacio húngaro como un elemento clave de la vida económica y social húngara

en un entorno libre, seguro e innovador. A través de medidas de protección eficientes basadas en la prevención, el objetivo principal es gestionar las amenazas y los riesgos que surgen y provienen del ciberespacio, así como reforzar la coordinación y las medidas gubernamentales.

- En **Italia** se propone un marco de referencia para Gestión de Riesgos basado en el emitido por NIST[20] que consiste en una matriz en la que se evidencian las funciones *Identificar, Proteger, Detectar, Responder, Recuperar* los riesgos, para cada una de ellas se determinan las categorías, subcategorías y las referencias informativas. Este marco de referencia se complementa con unos niveles de madurez y niveles de prioridad (Roberto & Montanari, 2015). El Gobierno italiano aprobó el nuevo Plan Nacional de Ciberprotección y Seguridad Digital que define nuevas directrices y objetivos operacionales para la implementación del Marco Estratégico Nacional para la Seguridad Cibernética (NSF). El nuevo plan se ha desarrollado de acuerdo con las directrices para la ciberprotección y la Seguridad Digital recomendadas por el Primer Ministro como responsable de la Ciber Arquitectura Nacional. El plan de acción se basa en medidas sustanciales que fortalecen la ciberarquitectura nacional, teniendo en cuenta que los datos confidenciales para fines de Seguridad Nacional no son exclusivamente administrados por el sector público, sino que están integrados con datos confidenciales de empresas privadas en sectores estratégicos. Por lo tanto, el nuevo plan de acción y gestión de crisis amplía el perímetro de las empresas que operan en áreas identificadas como críticas para la seguridad nacional (proveedores de servicios públicos y proveedores de servicios digitales), que estarán sujetas a nuevas obligaciones de notificación ante la ocurrencia de incidentes de seguridad identificados como amenazas a la seguridad nacional basadas en ciertos parámetros y umbrales. Las

20 https://www.nist.gov/

sanciones en caso de falla son bastante sustanciales. Las prioridades de la intervención de arquitectura nacional se describen como la identificación y actualización de medidas mínimas de Seguridad para ser implementadas en la administración pública y redes y sistemas de Infraestructura Crítica, la adopción de estándares de referencia, mejores prácticas y requisitos mínimos para la seguridad de redes y sistemas, la construcción de un sistema de auditoría de validación y para los organismos responsables de la emisión de certificados digitales, para autenticación y otros certificados digitales de valores.[21]

- En **Polonia**, se considera vital establecer un sistema de financiación de las tareas relacionadas con la protección del ciberespacio y se argumenta que la protección efectiva del espacio cibernético debe incluir la adopción de un marco legal para un Sistema Nacional de Protección del Espacio Cibernético, que se establezca una institución estatal que coordinará las actividades de otras entidades. Por otra parte, se pretende destinar recursos para hacer frente a las alertas y desarrollar un modelo de análisis y Gestión de Riesgos nacional (Strężyńska, 2016).

21 A este respecto, se transcribe del original en inglés de The National Cyber Security Strategy, published in 2015. "Is a high level policy statement from Government. It acknowledges the challenges with facilitating and enabling the digital economy and society. The strategy is based on key principles such as the rule of law, subsidiarity, noting that we are ultimately responsible for our own security, and proportionality in response to key risks and threats facing us. Key measures include:

- Formally establishing the National Cyber Security Centre, encompassing the national/governmental Computer Security Incident Response Team (CSIRT-IE) Its focus on the protection of critical national information infrastructure in key sectors such as energy and telecommunications.
- Delivering improved security arrangements, in partnership with Government Departments and Key Agencies involving situational awareness and incident management.
- Introducing primary legislation to formalise arrangements in law and to comply with EU requirements on capabilities, co-operation and reporting.
- Co-operating with key State Agencies, industry partners and international peers in the interests of protecting critical infrastructure, improving situational awareness and incident management along with facilitating education, training and public awareness initiatives".

- En el **Reino Unido**, el Gobierno cuenta con un marco de referencia gubernamental en Gestión de Riesgos (Service, 2017) en el que se tipifican y gestionan los riesgos asignando responsabilidades de acuerdo con el rol que cumplen dentro de la administración. El marco de referencia establece cuatro diferentes tipos de riesgo: *Internos, Externos, Proyectos principales, Estrategia*; tres elementos de Gestión de Riesgos: Construcción de bloques, actividades periódicas y procesos de rutina; finamente están los roles/responsabilidades garantizando que hay claridad en quien hace que dentro del contexto.

- **República Checa** ha tenido un éxito desigual en la implementación de una agenda integral de gobierno electrónico. Si bien la disponibilidad de servicios de gobierno electrónico fue del 56 % para los ciudadanos y del 100 % para las empresas en 2010, el uso real de los servicios de gobierno electrónico solo alcanzó el 29 % para los ciudadanos y el 94 % para las empresas en 2013, lo que indica una gran brecha el uso de servicios de gobierno electrónico por parte de los ciudadanos y las empresas. Esto probablemente se deba al hecho de que a todas las personas jurídicas se les proporcionó un "buzón de datos" gratuito pero obligatorio a partir del 1 de julio de 2009 en adelante. El buzón de datos funciona como una cuenta de correo electrónico normal, pero proporciona la autenticidad y la no negación de los datos almacenados (utilizando el algoritmo de función hash SHA-2), eliminando así la necesidad de un certificado separado para firmas electrónicas. Toda correspondencia oficial entre personas jurídicas y autoridades está restringida al buzón de datos. Como se considera que los mensajes no leídos que se entregan en el buzón de datos han sido leídos por el destinatario 10 días después de la entrega, las empresas no tienen más opción que cumplir con los procedimientos de gobierno electrónico relacionados con el uso del buzón de datos. Por el contrario, las personas físicas no están obligadas a utilizar el buzón de datos y, por consiguiente, menos del 1 % lo tienen. Los certificados para firmas electrónicas no los proporcionan las autoridades públicas y deben comprarse a enti-

dades comerciales, lo que se ha convertido en otro obstáculo para uso generalizado del gobierno electrónico por personas físicas. Por lo tanto, mientras que la República Checa ocupa el octavo lugar dentro de la UE en el uso del gobierno electrónico por parte de las empresas, ocupa el lugar 23 en la categoría correspondiente para las personas (Minárik, 2016).

La Agencia Nacional de Seguridad Checa también tiene un acuerdo sobre el Programa de Seguridad del Gobierno con Microsoft, según el cual, las partes pueden compartir e intercambiar información de Seguridad cibernética, lo que significa que la ANS tiene acceso a los códigos fuente y la documentación de los productos de Microsoft. Se ha celebrado un acuerdo de intercambio de información similar entre la ANS y Cisco. Con base en este memorando de entendimiento, estas dos entidades comparten información sobre ciberamenazas e intercambian información sobre las actuales tendencias de Seguridad cibernética y las mejores prácticas.

- En **Rumania,** el Gobierno propone un plan de gestión de riesgo alineado con las políticas de la Comunidad Europea; en primer lugar, proponen realizar la *Identificación, valoración y mitigación del riesgo;* posteriormente, la información que puede estar expuesta a un riesgo se clasifica en cuatro categorías, *Gestión y publicación de información, moderación, recursos y gestión de proyectos*. Se utiliza también una subcategoría de riesgos y finalmente, se plantean los riesgos específicos. De esta manera, se mapean los posibles riesgos y las acciones de mitigación correspondientes (Otniel, 2015).

. En **Rusia**, el presidente Vladimir Putin aprobó la Doctrina de Seguridad Informática en el año 2016, esta identifica la Seguridad cibernética, la privacidad y la Seguridad de la información como vitales para los intereses nacionales de Rusia y pretende formar la base de nuevos desarrollos en las políticas públicas y las relaciones públicas, así como mejorar los sistemas para la

protección de la Seguridad de la información. Entre los pilares de la nueva Estrategia de Gestión de Riesgos en Seguridad Digital se enfatiza en la promoción y protección de la privacidad de la información, el apoyo a las instituciones democráticas, el Estado y los mecanismos de interacción de la sociedad civil. De este modo, se pretende garantizar el funcionamiento sostenible e ininterrumpido de la Infraestructura Nacional de Información Crítica en tiempo de paz y tiempo de guerra y en respuesta a actos de agresión extranjeros, además de la promoción nacional e internacional de las políticas del Gobierno ruso en materia de Ciberseguridad y Defensa (The Ministry of Foreign Affairs of the Russian Federation, 2016).

- En **Suiza**, el Consejo Federal encargó al Departamento Federal de Defensa, Protección Civil y Deporte (DDPS) el 10 de diciembre de 2010, elaborar una Estrategia Nacional para la protección de Suiza contra los riesgos cibernéticos. Esta estrategia describe qué aspecto tienen estos riesgos, por ejemplo, qué tan bien Suiza está equipada para contrarrestarlos, dónde se encuentran las deficiencias y cómo pueden eliminarse de manera más efectiva y eficiente. La Estrategia para la Protección de Suiza contra los Riesgos Cibernéticos se dirige principalmente a las agencias federales y se elaboró en colaboración con representantes de todos los departamentos, varios operadores de Infraestructura Crítica, el servicio de proveedores de TIC, proveedores del sistema y el sector privado. La estrategia describe los roles de varios actores y modelos de colaboración requeridos para una mejor protección contra los ciberriesgos (Eidgenössisches Department für Verteidigung, 2012).

- En **Estados Unidos**, el presidente Donald Trump firmó la orden ejecutiva de Ciberseguridad[22], la cual hace énfasis en Ges-

22 https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

tión del Riesgo y resiliencia de Infraestructura Crítica, ciberdisuasión y desarrollo de la fuerza de trabajo cibernética y los procesos se alinean con la planificación estratégica, operativa y presupuestaria. Cada agencia del Gobierno debe adoptar los estándares de la *NationalInstitute of Standards and Technology* (NIST)[23] y enviar los documentos de Gestión del Riesgo a la Secretaría de Seguridad de la Casa Blanca. El último marco de referencia emitido por el NIST es el *Framework forImproving-CriticalInfrastructureCybersecurity* y se plantea en términos de identificar, valorar y responder al riesgo, priorizando decisiones respecto a la Ciberseguridad (Technology, 2017).

- **Canadá** al igual que Estados Unidos no tiene un marco de referencia pero sí cuenta con unas guías para la Gestión del Riesgo que sugiere una división de actividades en dos niveles: El nivel *Departamental*, en donde se establecen las actividades alineadas con el plan de seguridad de la organización y el nivel de *Sistemas de Información*, en el que se encuentran las actividades relacionadas con el ciclo de vida del sistema de información y se implementan los controles de Seguridad apropiados con el fin de mantener la continuidad del negocio (Moffa, 2012).

De acuerdo con el estado del arte analizado previamente en diferentes países del mundo de los cinco continentes, es evidente que la Gestión de Riesgos en Seguridad Digital es un tema de gran relevancia a nivel de Estado, por tal razón, es necesario involucrar a todas las entidades comprometidas: Fuerza Pública, academia, y organizaciones públicas y privadas para establecer unos lineamientos generales que permitan identificar las vulnerabilidades, amenazas y riesgos a los que se vería expuesta una nación, para finalmente, consultar a la población en general sobre sus intereses, necesidades y temores a los que se ven expuestos, de esta manera, se podrá es-

23 https://www.nist.gov/

tablecer un marco general de buenas prácticas que establezca tanto los deberes como las responsabilidades para mantener segura la información sensible que en caso de riesgo inminente, podría afectar la integridad humana o los bienes de los ciudadanos y/o organizaciones.

En ese sentido Colombia debe iniciar un trabajo colaborativo entre las diferentes partes para aprovechar la experiencia de los que ya han venido trabajando en el tema y a su vez adelantar e integrar a los demás actores que se han venido quedando rezagados en cuanto a la Gestión de Riesgos, con el propósito de que se adquiera conciencia de la importancia de proteger los activos de información y de resaltar la responsabilidad que cada uno tiene (organizaciones e individuos) sobre la información que maneja para prevenir, minimizar y evitar los riesgos latentes que se presentan ante un activo digital.

3. PERSPECTIVAS A FUTURO

Con base en la hipótesis de que para generar un marco de Gestión de Riesgos integral se requiere de la participación de todos los actores principales de la sociedad, se debe involucrar al sector de la academia, sector público, sector privado y Fuerza pública, teniendo en cuenta que estos sectores son claves como motor del desarrollo de cualquier país debido a su impacto e influencia en los diferentes sectores de la sociedad y al que de una u otra manera se encuentran vinculados todos los ciudadanos. De este modo, avanzando en el análisis realizado a nivel de Europa y América en el sector público se pretende dar una mirada holística de lo que se espera que continúe sucediendo en tema de Gestión de Riesgos, si se mantiene una evolución constante en este tema, en todos los países interesados en proveer una infraestructura física, y de servicios en un ambiente digital.

Si bien es cierto que existen coincidencias en el sector público sobre las necesidades y problemáticas que se pretenden abordar, las diferentes entidades del Estado difieren en la priorización que le dan a cada una de ellas. Por tal razón, se han creado políticas internas que den respuesta a esas prioridades identificadas y establecidas por cada organización que le permiten cumplir con su misión y visión, pero también se han generado cooperaciones con otras entidades del mismo sector para reaccionar ante cualquier eventualidad que requiera del concurso de todas las entidades involucradas, igualmente se establecen relaciones de confianza con fines estratégicos que permitan a las partes estar a la vanguardia en términos de tecnología, información y Seguridad Digital. Para poder generar dichas sinergias, se debe contar con diferentes perfiles profesionales no solo en materia de tecnología, sino en las diferentes ramas del saber que tengan algún tipo de injerencia en el actuar del medio tecnológico (abogados, ingenieros, economistas, etc.) ya que el entorno virtual ha permitido la apertura de diferentes mercados que requieren de conocimientos multi e interdisciplinares y se debe estar preparado para todo tipo de fenómeno que ocurra en Internet, tal como ocurrió con la aparición de la tecnología *Distributed Ledger Technology* (DLT) y *Blockchain Technology* (Svein Ølnes, 2017) y en particular con las aplicaciones y usos que se le puede dar, como es el caso de las criptomonedas (Antonopoulos, 2015), que han tenido un impacto importante en diferentes economías del mundo, ya que a partir de ahí se han generado oportunidades de negocio pero también riesgos asociados, no solo para inversores particulares, sino también para empresas y gobiernos.

En Colombia, se están haciendo esfuerzos importantes para avanzar en la disminución de la brecha digital que existe respecto a países desarrollados y se tienen como referencias de facto los estándares internacionales y la normatividad local entre ellas están las emitidas por NIST (Commerce, 2018), ISO (Standardization, 2018) y los documentos nacionales emitidos por el

Consejo Nacional de Política Económica y Social (Conpes, Departamento Nacional de Planeación, 2018), así como las normas emitidas por el organismo de estandarización nacional, Instituto Colombiano de Normas Técnicas (Icontec, 2018). De esta manera, se pretende avanzar en la consecución de los objetivos planteados a corto, mediano y largo plazo en temas de Gestión de Riesgos en Seguridad Digital. Por esto, siguiendo dicha normativa se han identificado algunos temas prioritarios a investigar entre los cuales se encuentran:

- Diseño de un Modelo integral de Gestión de Riesgos en Seguridad Digital, para el desarrollo de la economía digital de Colombia y servicios a los ciudadanos

- Marco normativo estableciendo políticas y protocolos en la protección de datos personales e identidad digital

- Definición de capacidades para el desarrollo de la gestión de ciberinteligencia e innovación

- Modelo de intercambio de información (Ley)

- Observatorio de riesgos de Seguridad Digital basado en *big data* para el análisis descriptivo, cognitivo y predictivo de amenazas vulnerabilidades e incidentes que involucre las partes interesadas (academia, sector público, privado, sociedad) para la efectiva toma de decisiones.

Las temáticas anteriores se pudieron identificar involucrando diferentes entidades del sector público y de acuerdo con la experiencia de sus funcionarios, se realizó la priorizar correspondiente.

4. CONCLUSIONES

En general, los países en diferentes continentes están efectuando importantes avances en el tema de Gestión de Riesgos de Seguridad Digital y Colombia también está haciendo lo propio, con el fin de hacer frente a las posibles amenazas en el ciberespacio y lograr la prosperidad social y económica del país.

Por tal razón, es necesario que los diferentes actores del Gobierno trabajen en conjunto para generar las políticas públicas apropiadas en temas de investigación, definiendo las líneas de interés que más impactan en cuanto al riesgo digital, según la visión particular de cada una de las entidades.

De acuerdo con el análisis realizado en otros continentes y también en el ámbito nacional, fue posible establecer el estado del arte en el que se evidenció el interés por involucrar diferentes sectores para establecer las mejores prácticas en términos de Gestión de Riesgos en Seguridad Digital, con el propósito de que las diferentes entidades, organizaciones y personas naturales apropien la tecnología y confíen en un sistema que provea los requisitos de Seguridad aceptables, dando así confianza a todos los usuarios para realizar transacciones en el medio digital, entendiendo como transacción cualquier intercambio de información realizado entre un emisor y un receptor.

Otro factor importante que se detectó es que se debe contar con personal experto en diferentes ramas, de manera que se pueda trabar de forma cooperativa y colaborativa entre equipos multi e interdisciplinares, para que la reacción sea mucho más efectiva y se pueda dar una respuesta acorde con las necesidades planteadas por el entorno, que en general, es un entorno hostil al haber intereses de por medio, tanto económicos como reputacionales, sociales, entre otros.

Después de identificar las temáticas prioritarias en el sector

público, se debe generar un modelo cíclico, en el que se evidencie que la Gestión de Riesgos, al igual que la Seguridad de la información, es un proceso continuo y no una actividad puntual que tiene un inicio y un final determinado, ya que cualquier cambio en la tecnología, en los usuarios, o en la misma información hace que cambie tanto el entorno como los riesgos asociados; de manera que se debe realizar una monitorización constante, que permita adelantarse a los eventos que puedan surgir y así prevenir, detectar y remediar la situación en aras de minimizar un impacto negativo sobre los activos de una sociedad, teniendo en cuenta que el análisis se realizó a nivel de gobierno.

En ese sentido, es necesario abordar las temáticas identificadas desde un punto de vista holístico con el fin de tener en cuenta todas las necesidades y establecer un marco de gestión común a todos los actores participantes a nivel Gobierno y continuar con el establecimiento de políticas, procedimientos y buenas prácticas de manera general, para sí, poder adaptar los modelos de gestión internos y cumplir con los objetivos propuestos en cada una de las entidades de acuerdo con su misión y visión, pero también con la capacidad de reaccionar en conjunto y estar alineados hablando el mismo lenguaje en caso de hallarse ante una situación de riesgo.

CAPÍTULO V

GESTIÓN DE RIESGO EN SEGURIDAD DIGITAL EN EL SECTOR PRIVADO Y MIXTO - CONTEXTO GENERAL[24]

Arístides Baldomero Contreras[25]
Escuela Superior de Guerra

1. INTRODUCCIÓN

La popularización del uso de Internet, aparte de la gran cantidad de beneficios que ha traído, ha proliferado una desmedida cantidad de riesgos en contra de las personas y las empresas, esta últimas más vulnerables día a día debido a que la mayoría de las actividades se vienen automatizando y requieren una conexión continua a Internet; síntomas vitales permiten definir y determinar que de la mano con las estrategias de negocios y para crecimiento interno del sector productivo, la Seguridad Digital y las Políticas públicas regionales que involucren la protección por riesgos del cibercrimen o la ciberdelincuencia, sustentadas en normas claras de Seguridad Digital y Ciberseguridad, serán aquellas que como parte integral de los planes de negocios y por

24 Capítulo de libro resultado del proyecto de investigación titulado "Gestión de Riesgos en Seguridad Digital" de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra, que a su vez hace parte de la línea de investigación "Seguridad Digital" del grupo de investigación 'Masa Crítica', reconocido y categorizado en (C) por Colciencias. Registrado con el código COL0123247, está adscrito a la Escuela Superior de Guerra de la República de Colombia.

25 Abogado con Especialización en Procedimiento Penal Constitucional, candidato a MBA y Máster en Supply Chain Management, Certificado en Riesgos bajo ISO31000 Risk Manager PECB. (Oficial de la Reserva Activa del Ejército Nacional). Investigador de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto". Patrocinado por el Patrocinado por el Ministerio de Tecnologías de la información y las comunicaciones.

supuesto del manejo de crisis y la continuidad de los mismos le permitirán salir avante en un mundo más interconectado.

La creciente transformación digital ha promovido el aumento del uso de las Tecnologías de la Información y las Comunicaciones en todos los aspectos de la dinámica económica y social. Esta situación también ha traído consigo nuevos riesgos asociados con la confidencialidad y protección de información, así como frente al resguardo de las infraestructuras cibernéticas que soportan los negocios explica la Asobancaria, 2018.

En el presente capítulo la preocupación inicia por el papel y la importancia del sector mixto y privado en las cifras que impactan el producto interno bruto (PIB) de cada uno de los países de la región, es un buen punto de partida para dilucidar cuáles son los productos que más aportan o los más representativos de la economía nacional, así las cosas se debería entender que este sector en forma representativa se oferta en manera muy importante como blanco del cibercrimen y que su Seguridad Digital, de la misma manera debería contar con un blindaje especial.

¿Pero es así? ¿Realmente el sector mixto - privado, cuenta con las medidas necesarias de Seguridad Digital? O ha tomado valor ¿Cuánto viene impactando el desarrollo de la productividad en algunos de los países de Latinoamérica, o cuál es el estado de las grandes empresas como blanco de campañas delincuenciales por la vía digital?

Una reflexión en que identificamos de inmediato la preocupación de un impacto o ataque generalizado, por ejemplo en los hospitales, el sector del comercio, los restaurantes, las infraestructuras críticas, los hoteles, sin dejar a un lado, el sector financiero, integrado por las corporaciones de ahorro y vivienda (CAV), los bancos comerciales, las corporaciones financieras, los almacenes generales de depósito (AGD), las compañías de financiamiento comercial (CFC), las compañías de leasing y las sociedades de servicios financieros como las fiduciarias, los comisionistas de

bolsa, las compañías de seguros, entre otras y las cuales son responsables de aportar un porcentaje cercano al 60 % del PIB.

Sin olvidar además el porcentaje adicional que proviene de otros renglones dela economía como: la explotación de minas y canteras; la electricidad, el gas y el agua; la construcción; el sector de transporte y almacenamiento; los servicios personales, los servicios del Gobierno y muchos más.

Ahora bien, de las partes y resultados ya identificados, la Política Nacional de Seguridad Digital de Colombia, aprobada el pasado 11 de abril de 2016 por el Consejo Nacional de Seguridad Digital, mediante la expedición del *Documento Conpes 3854* (2016), informó la necesidad de crear 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.

Para ello y con el fin de alcanzar este objetivo específico, el Gobierno nacional acorde con el *Conpes 3854* (2016), debería adelantar estrategias como:

- establecer mecanismos de participación activa y permanente de las múltiples partes interesadas en la Gestión del Riesgo de Seguridad Digital

- adecuar el marco legal y regulatorio en torno a la dinámica de la economía digital y sus incertidumbres inherentes

- identificar y abordar los posibles impactos negativos que otras políticas pueden generar sobre las actividades de las múltiples partes interesadas o sobre la prosperidad económica y social en el entorno digital

- generar confianza a las múltiples partes interesadas en el uso del entorno digital, y finalmente

- promover comportamientos responsables en el entorno digital en diferentes niveles de formación educativa.

Aspecto que abordaremos en particular más adelante y con ello entender el estado actual y que sirva de insumo para seguir generando instrumentos pertinentes con relación al cumplimiento de la política definida y la priorización del desarrollo de los planes futuros en la materia; conveniente y de gran interés que se identifiquen cuáles son los principales incidentes, amenazas y ataques contra la Seguridad Digital (tratados como los que se producen a la Seguridad cibernética y/o seguridad de la información) que están afectando a los países, reconocer sus principales blancos u objetivos y conocer los costos económicos que estos representan para el sector mixto – privado.

Cabe aquí recordar la Declaración sobre Seguridad en las Américas (2003) aprobada por el Consejo Permanente en su reunión ordinaria, celebrada el día 22 de octubre de 2003 y en la cual firmemente convencidos de que, en vista de los cambios profundos que han ocurrido en el mundo y en las Américas desde 1945, se tenía una oportunidad única para reafirmar los principios, valores compartidos y enfoques comunes sobre los cuales se basa la paz y la seguridad en el Hemisferio, declaro entre sus valores compartidos y enfoques comunes, literal e, que:

En nuestro Hemisferio y en nuestra condición de Estados democráticos comprometidos con los principios de la Carta de las Naciones Unidas y la Carta de la OEA, se reafirmaba que el fundamento y razón de ser de la Seguridad es la protección de la persona humana y que la Seguridad se fortalecía cuando profundizamos en su dimensión humana, pero también se expresó que las condiciones de la Seguridad humana mejorarían mediante la **promoción del desarrollo económico y social**, del cual como hemos leído en cifras anteriores son responsables las organizaciones del sector mixto – privado, las cuales aportan un porcentaje cercano al 60 % del PIB.

Además la Declaración sobre Seguridad en las Américas (2003) explicó que las amenazas, preocupaciones y otros desafíos a la seguridad en el Hemisferio son de naturaleza diversa y alcance multidimensional y el concepto y los enfoques tradicionales deben ampliarse para abarcar amenazas nuevas y no tradicionales, que incluyen aspectos políticos, económicos, sociales, de salud y ambientales, sumando por lo tanto que se debían incluir decisivamente los ataques a la Seguridad cibernética.

2. SITUACIÓN ACTUAL

Por su parte, tomando como ejemplo y en forma inicial el estado de la Seguridad Digital de Colombia, en el cual el nuevo blanco de los cibercriminales se determinó en el año 2017 y en forma clara que fueron las empresas, sector productivo de la economía; con el cambio en la selección de las víctimas, pasando del ciudadano común a las grandes empresas del sector público - privado, las cuales generan una mayor rentabilidad a la actividad criminal, explicó el Centro Cibernético Policial (2017).

Nótese que el estudio de *Impacto de los incidentes de Seguridad Digital en Colombia* y practicado por la Organización de los Estados Americanos, MINTIC y BID (2017) explicó que estudios de este tipo reflejaron y representan una iniciativa pionera en la región y poco frecuente a nivel mundial, ya que revela información sobre las amenazas para la Seguridad Digital de un país y su capacidad de defenderse ante las mismas que resulta difícil de recolectar.

El mismo informe sitúa al gobierno de Colombia en la vanguardia de la generación de conocimiento en el área de la Seguridad Digital que facilita el diseño y la implementación de políticas y que atiendan a los aspectos más débiles de escenarios reconocidos.

Pero el mismo informe cuando se pregunta a las organizaciones colombianas, si creen que están preparadas para hacer

frente a un incidente digital, un promedio simple del **37 %** de las empresas que participaron del estudio (empresas de los sectores Servicios, Industria y Comercio) explicaron que estaban preparadas para manejar un incidente digital, dejando por fuera el **63 %** que es un cifra preocupante.

De llamar la atención, entre las medidas más importantes que se pudieron identificar para asegurar las organizaciones colombianas frente a los incidentes digitales, es la identificación de un cargo con dedicación exclusiva para el manejo de este tipo de incidentes, este cargo es importante ya que les ayudará a las entidades a detectar, aislar y resolver incidentes rápidamente cuando ocurran explico la Organización de los Estados Americanos *et al*. (2017)

Por otro lado y para no dejar descartar y llamar la atención a la importancia del estado actual de los riesgos para la Ciberseguridad, explica el Foro Económico Mundial (2018) que estos riesgos también están aumentando tanto en su prevalencia como en su potencial desestabilizador. Los ataques contra las compañías casi se ha duplicado en cinco años y los incidentes que antes se consideraban extraordinarios son cada vez más comunes.

El impacto financiero producto de las violaciones de Seguridad cibernética está aumentando y algunos de los mayores costos de 2017 están relacionados con los ataques mediante programas de secuestro cibernético, que representaron el 64 % de todos los correos electrónicos maliciosos.

Algunos ejemplos notables incluyeron el ataque WannaCry, que afectó a 300 000 computadoras en 150 países, y NotPetya, que causó pérdidas trimestrales de USD 300 000 000 a varias compañías afectadas.

Otra tendencia creciente es el uso de ataques cibernéticos dirigidos a la infraestructura fundamental y los sectores industriales estratégicos, lo que nos lleva a temer

que, en el peor de los casos, los atacantes podrían desencadenar un colapso de los sistemas que mantienen a las sociedades en funcionamiento.

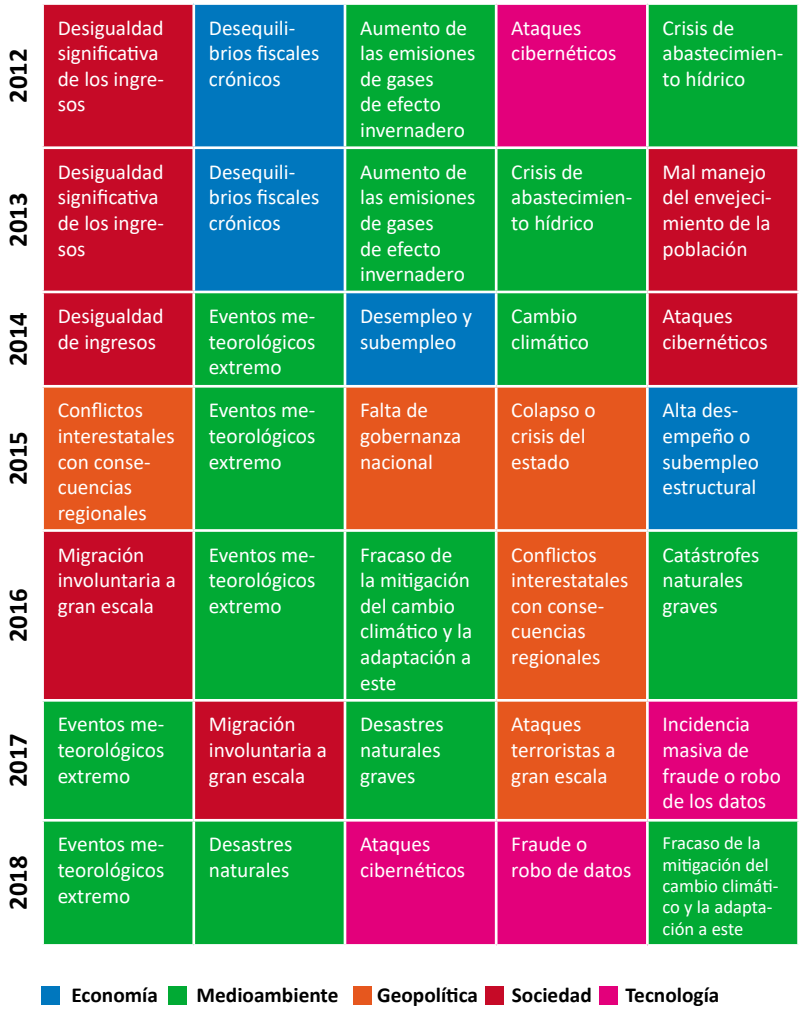


Ilustración 6. Los cinco riesgos globales en términos de probabilidad por el Foro Económico Mundial (2018).

Tomada de la Imagen IV: Panoramas de riesgos en evolución, 2008–2018. Informe de riesgos mundiales 2018, 13.a edición. Ginebra p. 6.

2.1. Estado y panorama de Latinoamérica en países acorde con políticas y estrategias nacionales de Seguridad Digital y cibernética.

Frente a la Seguridad Digital, América Latina y Caribe requieren mayores esfuerzos en Ciberseguridad, esto toda vez que la región presenta vulnerabilidades "potencialmente devastadoras" y donde Cuatro de cada cinco países carecen de Estrategia de Ciberseguridad resaltó el BID y OEA (2016).

Entonces, es menester mencionar algunos casos sobre el estado de adhesión en políticas de Seguridad Digital para la región.

- Colombia 2011 – 2016

El Consejo Nacional de Política Económica y Social del Gobierno de Colombia estableció la Política nacional de seguridad cibernética *Conpes 3701* bajo el auspicio del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el Ministerio de Defensa, el Departamento Nacional de Planeación y otras instituciones nacionales clave.

Además, en 2014 una Misión de Asistencia Técnica de la OEA ayudó al país a construir la capacidad con las partes interesadas para desarrollar marcos y políticas institucionales.

El Grupo de Respuesta de Emergencias Cibernéticas de Colombia (ColCERT) es una institución clave en Defensa y Seguridad cibernética y se muestra competente para la coordinación con otros organismos y el sector privado. En Colombia funciona un mecanismo de respuesta a incidentes cibernéticos específicos y los programas de Gestión del Riesgo han comenzado a surtir efecto.

Colombia cuenta como bien se mencionó, con Política Nacional de Seguridad Digital, aprobada en abril de 2016 al expedirse el Documento *Conpes 3854 (2016).*

Por otro lado, Colombia que fue el primer país de la región en tomar muy en serio este tema, ha captado la atención mundial, pero aunque esta información podría ser curiosa no lo es, debido a que Colombia se encontraba inmersa en una lucha interna contra las Fuerzas Armadas Revolucionarias de Colombia (Farc) durante varias décadas, una lucha que hace que las Fuerzas Militares y la Policía, en coordinación con el sector privado, defiendan y protegieran la Infraestructura Critica, física y virtual del país.

Por tanto, en la etapa final de su Política Nacional de Ciberseguridad y Ciberdefensa (Conpes 3701/2011), se formaron grupos de trabajo y se incluyeron a las instituciones del Gobierno nacional (Ministerio de Defensa Nacional, MinTIC, la Policía Nacional, etc.) y a las organizaciones del sector privado (representantes de los sectores de energía y comunicaciones, administradores de los dominios .co, universidades, etc.) con los cuales se creó un marco serio y coordinado que buscó proteger las infraestructuras críticas del país, denominado según el documento *Conpes 3854/2016* y desde el pasado 11 de abril de 2016 "la Política Nacional de Seguridad Digital".

En primer lugar, se estableció un marco institucional claro en torno a la Seguridad Digital. Para esto, se crearon las máximas instancias de coordinación y orientación superior en torno a la Seguridad Digital en el gobierno, y se establecieron figuras de enlace sectorial en todas las entidades de la rama ejecutiva a nivel nacional.

En segundo lugar, se crearon 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 fortaleció la Defensa y Seguridad Nacional en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos y por último, se siguen generando 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 está ejecutando desde el año 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.

- Brasil 2014

El país más grande de América Latina, también es el más digitalizado, y ha hecho la mayor inversión en TI de la región. También es el cuarto país con el mayor número de usuarios de Internet del mundo con más de 100 millones de personas conectadas a Internet, gracias a los incentivos del gobierno. La presidencia de la República aprobó́ el Marco Civil de Internet en abril de 2014, el cual plantea las reglas, los derechos y las obligaciones del uso de Internet, así́ como la protección de los datos.

- Panamá 2013

Desde mayo de 2013, el Gobierno de Panamá ha estado trabajando en la implementación de su Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructura Crítica (ENSC+IC), desarrollada por la Autoridad Nacional para la Innovación Gubernamental (AIG). Este documento, junto con un informe de posición titulado "La Resiliencia de la Infraestructura Crítica, Protección de Menores en Internet y Seguridad Cibernética", establece metas y diseña papeles y responsabilidades. Desde entonces, las entidades del gobierno han comenzado las etapas iniciales del desarrollo de planes internos de Seguridad cibernética

- Trinidad y Tobago 2013

En respuesta a una serie de ataques cibernéticos en 2011, el Marco de Políticas de Mediano Plazo de Trinidad y Tobago reconoció oficialmente tanto el papel que desempeñan las TIC en la promoción del desarrollo y el crecimiento económico nacional como la necesidad de implementar iniciativas efectivas de Seguridad cibernética para proteger esta infraestructura central. En diciembre de 2012 el Ministerio de Seguridad Nacional publicó una Estrategia Integral Nacional que detalla los riesgos cibernéticos del país y establece las funciones y responsabilidades de las entidades.

- Jamaica 2015

En 2013 el Gobierno de Jamaica no tenía en marcha políticas ni estrategias de seguridad cibernética. Dos años después, ya ha diseñado una Estrategia Nacional Integral, presentada el 28 de enero de 2015. Cuenta con un Grupo Nacional de Trabajo de Seguridad Cibernética, establecido bajo el Ministerio de Ciencia, Tecnología, Energía y Minería. El Programa de Se-

guridad Cibernética de la OEA y otras organizaciones internacionales han ayudado a Jamaica en el desarrollo de su CSIRT. Cabe destacar que a raíz de una serie de ataques cibernéticos contra sitios web del gobierno a finales de 2014, la OEA envió un equipo de expertos a Kingston para dar apoyo en la gestión de incidentes.

Los nuevos países que se han adherido a la formulación de políticas públicas en materia de Seguridad Digital en el 2017 son: Costa Rica, Paraguay, Chile, México, República Dominicana.

- Guatemala 2018

Pero estas se fundamentan y avanza según los pilares jurídicos de los países partes de la región, algunos de ellos han sumado a sus ordenamientos penales contemplar los delitos informáticos, la mayoría de los países en Latinoamérica, luego de la invitación han firmado su adhesión al Convenio sobre la Ciberdelincuencia o Convenio de Budapest.

"Convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional" (Convenio de Budapest, 2001).

Además, que el Convenio reconoce la cooperación entre el sector privado y los gobiernos, en aras de la necesidad de protección de "los intereses legítimos en la utilización y el desarrollo de las tecnologías de la información; estimando que la lucha efectiva contra la ciberdelincuencia requiere de una cooperación internacional reforzada, rápida y eficaz en materia penal".

En Latinoamérica los países firmantes son:

PAÍS	FECHAS
Argentina	5 de junio de 2018
Colombia	(En Proceso Interno)
Costa Rica	22 de septiembre de 2017
República Dominicana	17 de febrero de 2013
Panamá	5 de marzo de 2014
Paraguay	(En Proceso Interno)
Perú	(En Proceso Interno)

Tabla 2. países firmantes

Véase estatus extraído de la web oficial de Council of Europe del 23 de julio de 2018 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?desktop=true (Chart of signatures and ratifications of Treaty 185, Status as of 23/07/2018, Convention on Cybercrime)

Indica Miró (2012), que, para llegar a comprender el cibercrimen, para prevenirlo, es muy importante entender la forma en que las personas interactúan con el ciberespacio cada día e incluso a cada hora, donde lo hacen y el modo en que trabajan. Resalta que debemos pensar asimismo en la relación que guarda el uso del ciberespacio con los extensos patrones de la vida diaria.

Suma a sus comentarios que cualquier persona que trabaje de noche podría: "hacerse con contraseñas o utilizar los ordenadores de empresas que no estén bajo vigilancia, un padre que no supervise a su hijo adolescente durante el día o durante el viaje de fin de semana podría desconocer que se ha iniciado en el cibercrimen o que es víctima de este".

Señala Cohen y Felson (1979) que el crimen se produce durante los actos cotidianos del día a día, cuando se unen en el espacio y el tiempo un objetivo adecuado, un delincuente motivado y sin un guardián capaz de darle protección al primero.

Pues bien, como se ha señalado en las páginas anteriores el sector mixto – privado es de gran interés para los gestores de

la criminalidad digital, solo al revelar que más del 63 % de las organizaciones del sector mixto – privado explicaron que no estaban preparadas para manejar un incidente digital nos deja en desventaja y si sumamos que este tipo de organizaciones se encuentre en un país con falta de políticas se seguridad, se complementa como un espacio perfecto para la comisión del mismo.

Nos deja claro que al analizar en qué medida el ciberespacio se configura como un nuevo ámbito de oportunidad criminal obliga a repensar las estrategias de prevención de la delincuencia y de qué forma podemos adaptar las enseñanzas de la Teoría de las Actividades Cotidianas también tratada por Cohen y Felson (1979).

La Seguridad misma del gremio es un reto, ya sea por su importancia en la economía o por el papel que juega en el PIB de cada país, sumado a la aceleración y el grupo de motivos que nos llevan a cumplir los principios de la nueva revolución industrial y a la transformación digital para la prestación de los servicios.

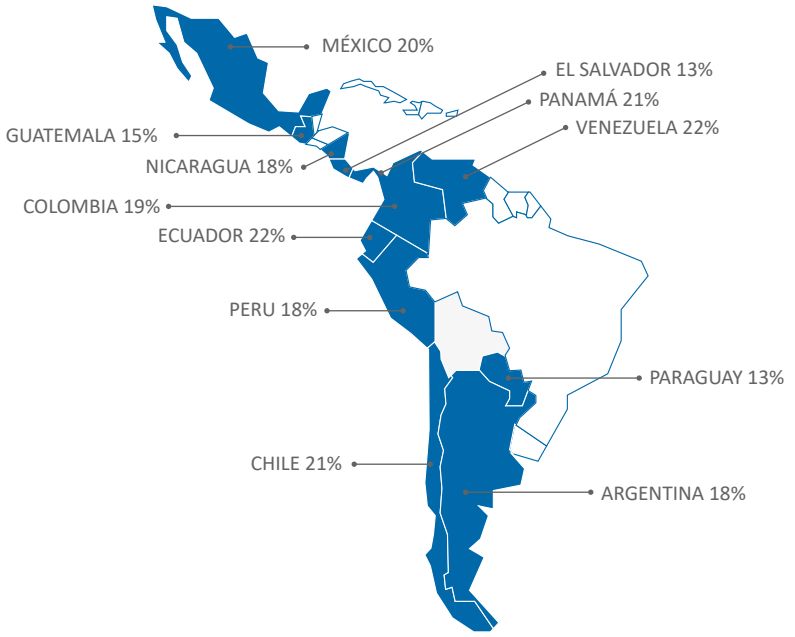
A la fecha la criminalidad digital sigue incrementándose, debo mencionar que esto obedece también a la falta de compromiso en la denuncia, hay suficientes razones para que el cibercrimen sea particularmente difícil de cuantificar y cuando obedece en las empresas la necesidad de proteger la reputación se cierra la oportunidad de la no repetición en el sector al cual pertenezca la organización afectada.

Debemos aunar esfuerzos y mantener un enfoque actualizado, en equipo y de transferencia de información, sucede a menudo que la víctima (persona u organización) no se da cuenta del ataque al que fue expuesto, o cuando ya lo hace lo entiende demasiado tarde para poner en conocimiento, estos comportamientos llevan en general a un apoyo indirecto de la criminalidad digital.

2.2. El inminente crecimiento de las infecciones y ataques a la Seguridad Digital en la región.

A medida que pasa el tiempo, cifras evidentes resultan la importancia de la Seguridad Digital, al menos tres de cada cinco empresas en la región sufrieron por lo menos un incidente de seguridad, estando en el top la infección con códigos maliciosos (45 %). La mitad de ellos aparecen relacionados al *ransomware*, es decir que al menos una de cada cinco empresas encuestadas en toda Latinoamérica fueron víctimas del secuestro de información, explica ESET Latinoamérica (2018).

El siguiente grafico identifica el porcentaje de infecciones y no existe una gran diferencia entre las empresas de cada país, siendo Ecuador el que tiene un mayor índice de infecciones de *ransomware* y El Salvador el que tiene el menor.



Gráfica 7. Infecciones de *malware* por país. ESET Security Report Latinoamérica 2018

De la misma manera y según Kaspersky Lab, registró más de 746 mil ataques de *malware* diarios durante los últimos 12 meses en América Latina, lo que significa **un promedio de 9 ataques de *malware* por segundo**. Además, los ataques de *phishing* – correos engañosos para el robo de la información personal de los usuarios– han sido constantes en la región, principalmente en Brasil.

Los resultados, presentados durante la Octava Cumbre de Analistas de Seguridad para América Latina que se está realizando en la ciudad de Panamá, demuestran que toda la región ha experimentado una considerable cantidad de ciberamenazas, con la gran mayoría orientada al robo de dinero.

Hubo un incremento del 60 % en ataques cibernéticos en la región, donde Venezuela registra el mayor número de los ataques en proporción a su población con un total de 70.4 %, seguido por Bolivia (66.3 %) y Brasil (64.4 %). Al igual que en 2017, Brasil continúa encabezando a los países latinoamericanos en términos de alojamiento de sitios maliciosos ya que 50 % de los hosts ubicados en América Latina que se utilizaron en ataques a usuarios de todo el mundo está ubicado en este país.

Según los datos de la empresa, la mayoría de estos ataques ocurre en línea, mientras se está navegando, descargando archivos o cuando reciben adjuntos de correos electrónicos engañosos y afectan más a los usuarios domésticos que a empresas. Sin embargo, la investigación también reveló que las empresas son más propensas a ataques vía email (60 %) y vectores *offline* (43 %); es decir, través de USB contaminadas, la piratería de *software* u otros medios que no requieren el uso obligatorio del Internet.

El año 2017, Brasil también estuvo dentro de los 20 países más atacados a nivel mundial. Esto se debe, en gran parte, a que los cibercriminales utilizan el correo electrónico, mensajes de SMS, llamadas telefónicas, anuncios en redes sociales, entre

otros, con nombres de empresas conocidas, lo que hace que los usuarios no desconfíen de esos mensajes, aumentando la probabilidad de que estos sean compartidos con su red de amigos (Assolini, 2018).

Y es que ya el aumento de los ataques cibernéticos en América Latina se había alertado que fue de un 59 % entre 2016 y 2017. Además, explica que cada vez son más diversos, sofisticados, potentes y con mayor alcance e impacto, así lo deja saber también en Colombia, el informe del Centro Cibernético Policial (2017), en el cual el cibercrimen del país aumentó un 28.3 %.

Aunque en Colombia, el Estado ha avanzado en la definición de una Política Publica de Ciberseguridad y en el fortalecimiento institucional, debido a los enormes impactos que podría tener un incidente en la Seguridad Digital de las organizaciones, no solo en términos netamente monetarios sino en perdida de información y amenaza sobre la reputación, todas las instituciones públicas y privadas deben trabajar en el fortalecimiento de sus capacidades para anticiparse a las ciberamenazas.

Resalta la Asociación Bancaria y de Entidades Financieras de Colombia, Asobancaria (2018) en cuanto a los esfuerzos por la articulación de políticas públicas para la protección ante los ciberataques o actividades que expongan nuestra Seguridad Digital: "Es previsible que la expedición de esta regulación acelere los avances en la constitución de un Sistema de Gestión de Riesgos de Ciberseguridad e implique reorganizaciones al interior de cada institución para fortalecer sus capacidades frente a las amenazas cibernéticas".

El sector privado y mixto como motor de la economía, mientras en la mayoría de los delitos tradicionales y para obtener una buena rentabilidad se hacía necesario un mayor esfuerzo superior, en los delitos informáticos de la nueva era, el esfuerzo es mínimo y la recompensa siempre es alta, Centro Cibernético Policial (2017).

Por ello las dinámicas del cibercrimen y su constante evolución exponencial, han propiciado que delincuentes que hasta hace poco actuaban de manera aislada, sin coordinación y con un alcance local, constituyan en la actualidad organizaciones trasnacionales complejas de cibercrimen.

Panoramas internacionales como el de Estados Unidos de América nos ayudan a dimensionar el alcance del acceso a la Internet y del ciberespacio, reconocido en forma asertiva y preocupante como una potencial sorpresa al evaluar las amenazas de la seguridad nacional de los próximos años, y que seguirán en aumento y más allá todavía de lo imaginado, ya que miles de millones de dispositivos digitales nuevos estarán conectados, con relativamente poca seguridad incorporada, y tanto los estados nacionales como los actores malignos se volverán más valientes y mejor equipados en el uso de herramientas cibernéticas que cada vez están más extendidas (Coats, 2018).

Por ende, el compromiso a dimensionar en el sector mixto y privado, se debe conectar con las necesidades y las nuevas prestaciones de las nuevas tecnologías, evaluando y motivando sobre las preocupaciones en los nuevos riesgos, so pena de encontrarse como organizaciones donde no se cuenta con procesos de seguridad, o donde no se plasman dentro de sus panoramas de riesgos las nuevas estratégicas o *Modus operandi* delincuencial, la evaluación asociada al cibercrimen, el ciberterrorismo, ciberactivismo o el ciberespionaje, podemos dar a entender que requerirá mayor acción y participación desde la sociedad y más aún desde el sector productivo.

3. SECTOR EN EL FUTURO

Tal y como lo explica el Centro Cibernético Policial (2017), la lógica de que esta "novedad" dure tanto, es la revolución de

las TIC, como concepto amplio, abierto y dinámico que engloba todos los elementos y sistemas utilizados en la actualidad para el tratamiento de la información, su intercambio y comunicación en la sociedad actual, se enmarca bajo el fenómeno del cibercrimen que no ha terminado todavía, ni lo hará en mucho tiempo, lo que supone que la cibercriminalidad o delincuencia asociada al ciberespacio y la Seguridad Digital seguirá evolucionando en las próximas décadas.

3.1. Retos frente a los delitos informáticos en el sector mixto – privado

La red informática se caracteriza por prestar un servicio de comunicación que no reconoce fronteras, día tras día los negocios y en especial la relación de oportunidades corporativas trasciende a escenarios digitales para lograr objetivos estratégicos ante la competencia.

La digitalización es ahora una mega tendencia pero ¿ dónde queda la Seguridad Digital de esta? Hay millones de dispositivos conectados a Internet que permiten hacer las cosas de forma muy distinta y fácil, más clientes necesitados de servicios y productos. Toda vez que el llamado a las empresas es emprender esta revolución y observando que lo que se requiere es aporte de conocimiento para que sean más globales y eficientes, surgen grandes interrogantes.

¿Están realmente las organizaciones capacitándose e implementado actividades bajo las nuevas tendencias y retos de la Seguridad Digital?

Este es el primer reto que deben evaluar las Empresas, si la respuesta es afirmativa en ese caso, se suma a un nuevo desafío ¿Están preparadas las empresas del sector mixto – privado, en la implementación de plataformas que brinden seguridad de sus servicios para lograrlo?

Descrito en la Comunicación oficial de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, la cual resalto la necesidad de creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos (Comisión de las comunidades europeas, 2000).

> Las infraestructuras de información y comunicación se han convertido en una parte crucial de nuestras economías. Desafortunadamente, estas infraestructuras tienen sus propias vulnerabilidades y ofrecen nuevas oportunidades para la delincuencia. Estas actividades delictivas pueden adoptar una gran variedad de formas y pueden cruzar muchas fronteras. Aunque, por diversas razones, no existen estadísticas fiables, no cabe duda de que estos delitos constituyen una amenaza para la inversión y los activos del sector, así como para la seguridad y la confianza en la sociedad de la información. Ejemplos recientes de denegación de servicio y ataques de virus han causado grandes perjuicios financieros, puede actuarse tanto en términos de prevención de la actividad delictiva, aumentando la seguridad de las infraestructuras de información, como garantizando que las autoridades responsables de la aplicación de ley cuenten con los medios adecuados para intervenir, respetando plenamente los derechos fundamentales de los individuos (Comisión de las comunidades europeas, 2000).

Ello supone, que toda prestación de servicios digitales deberá ofrecer soluciones ante uno de los retos principales, denominado “Confianza del cliente o del usuario digital” paradigma de prevención que enfrenta la nueva clase de delitos digitales y/o tecnológicos, bajo el alcance de las normas internacionales en la materia y las políticas públicas de cada país.

Casos a analizar nos pueden permitir vislumbrar en forma precisa, cuáles son los retos puntuales que la regulación Colombiana y que la Jurisprudencia en la materia posicionan hacia el sector.

Estos retos, sin el ánimo de cerrar la brecha a más posibilidades, pueden detallarse así:

1. **Seguridad de los servicios que ofrece y de las operaciones que permite realizar en relación con las plataformas digitales.**

2. **Seguridad como uno de los deberes significativos en la relación empresa – cliente.** La obligación de Seguridad puede considerarse como aquella en virtud de la cual una de las partes del contrato se compromete a devolver al otro contratante, ya sea en su persona o en sus bienes, sanos y salvos a la expiración del contrato, pudiendo ser asumida tal obligación en forma expresa por las partes, ser impuesta por la ley, o bien surgir tácitamente del contenido del contrato a través de su integración sobre la base del principio de buena fe.

3. **Reconocimiento de partes débiles a los clientes en toda relación de consumo,** y por ende que el ordenamiento jurídico promueva su protección y exija a las entidades un proceder consonante con el interés colectivo trascendente de protección al consumidor que emana de lo estatuido por los *Artículos 78* y *335* de la Constitución Política, lo que justifica la serie de obligaciones, cargas y conductas exigibles a dicho profesional, amén de un régimen de responsabilidad diferente del común.

4. **Necesidad de entendimiento de la Teoría del riesgo creado.** "La teoría del riesgo, impregnada por el valor moral de la solidaridad, parece sobre todo inspirada por

> la equidad: Por su actividad, el hombre puede procurarse un beneficio (o, al menos, un placer). Es justo (equitativo) que en contrapartida él repare los daños que ella provoca. Ubi emolumentum, ibi onus (ahí donde está la ventaja, debe estar la carga) (Díez L., 1999).

Su fundamento, según el autor precitado, resulta "del poder que tenía el responsable de evitar el daño. O para decirlo de otra manera por vía de una expresión a la cual nosotros adherimos y que empleamos usualmente, en su dominio; dominio que él tenía o, al menos, habría debido normalmente tener, de su actividad, así como de los hombres o de las cosas por las que él responde" (Trigo, y López, 2004).

Para lo cual, en su aplicación a las actividades del sector mixto o privado, se debe sostener que la relación existente entre el cliente y la empresa, requiere un intercambio continuo de confianza, a tiempo en que también determina la reciprocidad de esfuerzos en la tarea de evitar posibles daños por descuido o incumplimiento de las obligaciones contractuales de las partes, que con ello tendrá por entendidas también, las que le impongan como cargas por la ley a través de la presunción de responsabilidad.

5. **Las nuevas tecnologías y el riesgo de la actividad empresarial en medios digitales.** Afianzado bajo el concepto y la premisa de la modernización de la distribución de productos y servicios, lo que determinó el paso de las oficinas físicas a la atención al cliente por otros canales transaccionales como los cajeros electrónicos, los sistemas de audio respuesta, los centros de atención telefónica o *call center*, los sistemas de acceso remoto para clientes (RAS), el Internet y, recientemente, las aplicaciones en dispositivos móviles.

Estas últimas que en efecto requieren de rigurosos esquemas

de seguridad y protección de la información que por ellos circula, pues a través de estas se realiza la disposición de los recursos monetarios de los clientes.

En ese sentido, se ha dicho que la "difusión de la informática en todos los ámbitos de la vida social ha determinado que se le utilice como instrumento para la comisión de actividades que lesionan intereses jurídicos y entrañan el consiguiente peligro social…"

6. **Mayores exigencias, cargas y deberes según la actividad a desarrollar en el ambiente digital.** Como lo ha explicado la Corte Suprema de Justicia, Sala de Casación Civil de la Republica de Colombia, al decidir recurso de reposición el pasado diecinueve (19) de diciembre de dos mil dieciséis (2016) SC18614-2016 - Radicación No 05001-31-03-001-2008-00312-01 Magistrado Ponente Ariel Salazar Ramírez.

"El riesgo, entonces, se materializa con el ofrecimiento a los clientes de una plataforma tecnológica para realizar sus transacciones en línea, la cual puede ser vulnerada por delincuentes cibernéticos a través de diversas acciones, atendida la vulnerabilidad inherente a los sistemas electrónicos".

No obstante, el uso de este lleva ínsito el riesgo de fraude electrónico, el cual es de la institución financiera precisamente por la función cumplida por las instituciones financieras y el interés general que existe en su ejercicio y la confianza depositada en él, lo que determina una serie de mayores exigencias, cargas y deberes que dichas entidades deben cumplir con todo el rigor; por el provecho que obtiene de las operaciones que realiza; por ser la dueña de la actividad, la que **- se reitera -** tiene las características de ser profesional, habitual y lucrativa; y además, por ser quien la controla, o al menos, a quien le son los exigibles los deberes de control, seguridad y diligencia en sus actividades, entre ellas la de custodiar dineros provenientes del ahorro privado.

Por eso, por una parte las instituciones financieras están compelidas a adoptar mecanismos de protección de los datos transferidos en relación con sus usuarios, a través de los cuales pueda prevenirse la defraudación, pues para el momento en que estos son detectados, generalmente, ya se ha causado el daño patrimonial, y por otra, están sujetas a la responsabilidad que acarrea para ellas la creación de un riesgo de fraude que afecta a sus clientes, a disposición de los cuales ha dispuesto su plataforma y recursos tecnológicos.

3.2. Seguridad y mantener la confianza en el sector mixto – privado.

Sumado a lo anterior, la **"Seguridad y Mantener la Confianza"** y que esta se apropie y se mantenga alineada con el impacto de los ciberataques, trae un cuestionamiento muy importante a realizar.

¿Cómo contar la Seguridad Digital necesaria, como proteger nuestros activos claves y las operaciones? Reto para identificar las nuevas amenazas y a las que se está expuesto, la evaluación y pruebas para saber que proteger, sumado a la resiliencia digital y cibernética para saber dónde se es vulnerable.

Reconocer la necesidad de contar con enfoques más alineados en lo que más le importa a cada negocio y al impacto de los ciberataques, el sector mixto – privado por su carácter de importancia en la cadena de valor e impacto en (PIB) Producto Interno Bruto de los países, nos obliga a realizar enfoques basados en Riesgos, direccionar estrategias cibernéticas e inversión, acorde a las capacidades cibernéticas detectadas y que proporcionen la mejor protección a los activos claves y las operaciones previamente establecidos.

Recordemos que con los datos y la transformación digital, ahora en el corazón de la operaciones y las nuevas oportunida-

des que nos ofrece la apertura del mundo con la virtualización; la Seguridad Digital y cibernética deberá gestionarse, dotarse de recursos e integrarse adecuadamente, para **"mantener la Confianza"** y permitir el éxito.

El uso de los datos significa conectarse con un mundo más interconectado, la Seguridad Digital es necesaria, deja en claro como estamos reduciendo el riesgo y nos permite un cambio radical en los recursos y los controles, prioriza estos para reducir pérdidas y establece una Estrategia Cibernética Personalizada.

"No debe perderse de vista que el paradigma sobre el que descansan la nueva generación de delitos informáticos" o con ausencia de Seguridad Digital, "Se halla en el valor estratégico asignado a la información (los datos), y la respectiva protección de los sistemas de transmisión de dichos datos". Así mismo, "La seguridad no se trata solamente de una solución tecnológica, ya que también hay un componente humano que es necesario proteger".

El primer paso o característica de las grandes empresas o de las representaciones de organizaciones transnacionales, cuando se realiza un proceso laboral o de inducción a un nuevo empleado, es la entrega de un artículo electrónico digital conectado a la Internet.

ESET Latinoamérica menciona que de acuerdo con encuestas realizadas en Latinoamérica por parte de su organización.

> Solamente el 30 % de los usuarios utiliza una solución de seguridad en sus dispositivos móviles, a pesar de que más del 80 % reconoce que los usuarios son los que tienen la mayor cuota de responsabilidad al momento de caer en engaños por no tomar consciencia ni educarse sobre las diferentes estafas (ESET, 2018).

Ello trae un importante consideración de nuestro continente, la cibercriminalidad y los retos de su prevención van ligados directamente a las diferentes medidas que sean establecidas para que la decisión de actuar del cibercriminal, este valora el esfuerzo necesario que va a tener que realizar para cometer el delito, este agresor potencial ya reconoce que las pequeñas y mediana empresas son blancos importantes y llenos de información vital con grandes utilidades y menor Seguridad.

En resultados obtenidos de investigaciones y encuestas, se revelo que hay una consolidación de la función de gestión de ciberriesgos y Seguridad de la información, los ejecutivos responsables de administrar la seguridad de la información consideran que aún no cuentan con recursos suficientes y son conscientes que tienen un largo camino por recorrer.

Entre los mayores desafíos a conocer por parte de las organizaciones y en particular las del sector mixto – privado en Latinoamérica, se destacan en la implementación de capacidades de monitoreo de riesgos y de respuesta ante incidentes y brechas de seguridad de la información. "Esto resulta de relevancia considerando que 4 de cada 10 organizaciones han sufrido una brecha de seguridad en los últimos 24 meses" (Deloitte, 2016).

El camino para que las empresas del sector mixto y privado se conviertan en organizaciones adaptadas a los riesgos de Seguridad Digital, debe iniciarse a partir de la toma de conciencia y en los altos niveles directivos y ejecutivos de la organización, reconocer las ciberamenazas propias del nuevo ambiente digital de negocios, hablar e incluir en los presupuestos organizacionales cifras importantes para atender lo que a la fecha, ya es un flagelo que genera grandes pérdidas. Comprender el nivel de exposición y qué se puede hacer para mejorar, es el primer paso que los Ejecutivos y encargados de gestionar los riesgos digitales deben dar.

Uno de los elementos que pueden conformar el perfil y la oportunidad delictiva del cibercriminal va asociado al ámbito de oportunidad y a la perspectiva preventiva adoptada; justamente y en desarrollo de la presente investigación, en el año 2018 los países de Guatemala y República Dominicana presentaron sus estrategias nacionales de Ciberseguridad, sumado a ello ya son 10 países de la Región que han adoptado procesos para protegerse en el ciberespacio, un esfuerzo conjunto de gobierno, sector privado y sociedad civil, y con amplia participación y apoyo del Programa de Ciberseguridad que ahora trabaja con todos los países de la Organización de Estados Americanos (OEA).

La velocidad con la que aparecen las nuevas tecnologías, los nuevos reportes de ataques, las familias de *malware* o las fallas de seguridad con impacto global, hacen de la seguridad un desafío cada vez más importante para las empresas, los gobiernos y los usuarios alrededor del mundo, si bien es cierto en la actualidad se invita a las pequeñas, medianas y grandes empresas a explorar nuevos espacios y a descubrir ideas innovadoras sobre los productos o servicios que cada empresa ofrece, se les invita a la innovación, a nuevos formatos de planeación estratégica para lograr mejores resultados, **¿Dónde y cómo se habla de la Seguridad para estos procesos?**

Es importante reconocer cada uno de los interrogantes que se plantean en cada espacio de reflexión, los cuales nos enmarcan en la medida de evaluación “Digitalización Vs Migración Segura, ¿es oportuna y consecuente en forma apresurada?”

4. CONCLUSIONES

4.1. Supervivencia organizacional bajo una gestión oportuna de Seguridad Digital.

Nos quedan solo retos en la consolidación de la Seguridad Digital, la privacidad y los secretos empresariales, el sector mixto privado debe proteger sus ventajas competitivas, conocer y reconocer las amenazas cibernéticas que más se presentaron en los países de la región. Reconocer los tópicos de la consolidación del *Crime as a Service*, el cual como riego y amenaza es la modalidad en la cual se pone a disposición servicios, generalmente a través de la web, para que cualquier persona sin conocimientos profundos en tecnología los pueda contratar.

Al hablar de controles de Seguridad, probablemente sean muchos los que piensen en contar con alguna solución de Seguridad o tecnología de protección, pero pocos se plantearan la opción de incluir políticas y planes para gestionar la seguridad de la información. Y toda vez que esto último se ve reflejado en empresas de Latinoamérica, la tecnología no lo es todo a la hora de hablar de Seguridad, sino que deberá complementarse con una adecuada gestión, concientización y capacitación; y es en este punto donde hallamos las mayores diferencias y los principales riesgos.

Quizá uno de los puntos más débiles en cuanto a Seguridad Digital son las tecnologías de Seguridad relacionadas con los dispositivos móviles pues estas en su mayoría no cuentan con soluciones de seguridad para este tipo de equipos.

Otro punto que también resulta preocupante y que cabe destacar, es la baja adopción de tecnologías, como las que permiten hacer administración de parches y actualizaciones de software. Así, habiendo mencionado que 2017 fue histórico

en cuanto a la cantidad de vulnerabilidades reportadas, surge como un aspecto esencial para la protección tener las herramientas que permitan mantener los parches y las actualizaciones al día.

El elevado número de vulnerabilidades reportadas se encuentra acompañado del crecimiento en la cantidad de dispositivos IoT Internet de las cosas (en inglés, Internet of *Things*, abreviado IoT; IdC, por sus siglas en español, concepto que se refiere a la interconexión digital de objetos cotidianos con Internet.

Alternativamente, en Seguridad Digital la constante implementación del Internet de las cosas, que es la conexión de Internet con más objetos que con personas, seguirá llamando la atención a una mejora continua de los procedimientos, esto debido a su capacidad de procesamiento, pues pueden ser utilizados para realizar algún tipo de ataque o acceder a las redes a las que están conectados, además, porque la fuga de información fue un incidente bastante recurrente durante los últimos años.

Bajo los aportes anteriores, un llamado de atención y de importante inversión es necesaria en las empresas del sector mixto - privado, la supervivencia es un reto que de solo mirar hechos ocurridos como en Chile, donde recientemente se dio a conocer el caso de una estafa informática que afectó al Banco de Chile y donde un empleado realizó durante al menos un año transferencias no autorizadas por valor de 475 millones de pesos chilenos (cifra que supera los 700 mil dólares) simulando que se trataba de actividades laborales; y banco en el cual cabe destacar que se mencionaba entre las noticias por ciberataque, que también sufrió el 24 de mayo de 2018 un importante robo y en el que cibercriminales internacionales se llevaron mediante transferencias bancarias, cerca de 10 millones de dólares en lo que fue una operación sofisticada que incluyó la introducción de un código malicioso.

4.2. ¿Entonces que sumar a esta importante reflexión?

4.2.1. *¿Existen las amenazas internas?*

Cuando hablamos de medidas de Seguridad no solo nos referimos a las que se deben tener en cuenta para evitar ataques a la Seguridad Digital provenientes del exterior, sino también del interior de la empresa, organización o institución. Y es que puertas para adentro, una entidad, como puede ser en este caso un banco o cualquier entidad que maneje dineros o transferencias, debe tomar las precauciones suficientes ante la posibilidad real de que exista una amenaza interna.

La Ciberseguridad ha pasado de ser arbitraria y atemorizante, a ser un enemigo casi estándar en el arte de los negocios modernos. Ahora que la mayoría de las organizaciones han aceptado el axioma que algún nivel de vulnerabilidad de datos es universal, muchos se están graduando en una era de comprensión, preparación y receptividad.

Cómo se ejecutan en estas variables se ha convertido en una característica distintiva entre los que están listos para lo inevitable y para aquellos que están destinados a ser noticia de primera plana. Las organizaciones pueden tomar una amplia variedad de pasos o decisiones, que abarcan políticas, educación, liderazgo y tecnología, para combatir una amenaza que ha cautivado tanto a las comunidades profesionales como a las comerciales.

En este sentido, la realización de auditorías internas es una gran herramienta para establecer un diagnóstico acerca del estado de la Seguridad de cara a las puertas adentro de la organización, la siguiente recomendación suma a importante medida de prevención.

4.2.2. *Constante migración al mundo digital con interés y preparación hacia las nuevas amenazas digitales.*

Mencionar entonces que el conglomerado de organizaciones migran actualmente a lo digital, es una realidad y por ende bajo las premisas de la Organización de Estados Americanos OEA, que en pasado Reporte de Seguridad Cibernética e Infraestructura Critica de las Américas (2015) referente a las transformación y nueva generación industrial, explico que el interés de la comunidad de la Seguridad para analizar y descubrir nuevas vulnerabilidades de los sistemas de automatización industrial, en particular de las infraestructuras críticas, ha crecido rápidamente.

Si bien este interés comenzó en casi todas las conferencias de Seguridad importantes de 2013 y 2014, se ha hablado mucho de los ataques perpetrados contra los sistemas de control y automatización.

También se ha publicado mucho sobre este tema; asimismo, los proveedores están adaptando sus tecnologías para brindar "nueva" protección a estos sistemas. Sin embargo, lo más importante es el hecho de que los principales medios de comunicación han reportado un número importante de ataques que afectan principalmente a la producción y distribución de petróleo, gas y energía.

Y América Latina no ha sido la excepción; existe un gran interés por investigar las posibles debilidades y los ataques sufridos. Los países latinoamericanos han estado siguiendo esos temas muy de cerca, aunque tienen menores presupuestos que los de los países europeos y Estados Unidos.

CONCLUSIONES FINALES

A lo largo de los capítulos presentados en este libro se ha evidenciado la importancia para cada uno de los sectores de poder medir y mitigar el riesgo digital. Para cualquier economía, Internet amplía en gran medida los mercados de productos y servicios y por ello su importancia. Las partes interesadas reflexionan sobre la necesidad de una mayor integración entre la Ciberseguridad y los esfuerzos de desarrollo de la resiliencia. La resiliencia está surgiendo como la estrategia para abordar el cambio y la incertidumbre en un conjunto cada vez mayor de sectores, escalas y plazos. La resiliencia ofrece una visión de equilibrio de los sistemas y cómo podría responder a diversas circunstancias. A partir de ello y usando el análisis de riesgos, el problema del riesgo desde una perspectiva clásica se compone de la amenaza, vulnerabilidad y consecuencia, donde reduciendo la amenaza o la vulnerabilidad se concluye que la consecuencia es pequeña. Ahora bien, se sabe que no existe ningún sistema cien por cien seguro y siempre existirá la probabilidad de ocurrencia de un efecto de riesgo o de desorden (Entropía de Shannon) que se puede ver reducido a un equilibrio producido por la resiliencia.

Reducir la amenaza de Ciberseguridad significa centrarse en prevenir o impedir que el adversario actúe es decir que los carteles del ciberespacio tomen control. Esto a través de la óptica de un fortalecimiento jurídico complementa la reducción de la amenaza en la ecuación del riesgo. Evitar que el adversario actúe puede incluir la aplicación de la ley, la diplomacia, la Inteligencia o los esfuerzos militares para neutralizar a las personas o sus herramientas. Disuadir al adversario de actuar podría incluir una gama aún más amplia de opciones, dependiendo del adversario en particular.

Las tendencias actuales hacia la digitalización, la automatización y la interoperabilidad no necesitan excluirse mutuamente de la Seguridad. Sin embargo, el desafío de la Ciberseguridad solo puede abordarse de manera efectiva al comprender completamente la amplia gama de vectores de amenazas. Incluso entonces, estas preocupaciones solo se pueden resolver eficientemente al buscar las mejores opciones para reducir cada uno de los tres factores de riesgo.

Un elemento fundamental dentro de esta visión resiliente que se adiciona en la ecuación es una ciudadanía educada en el ámbito ciber, es decir que el individuo sea y deba ser un agente activo de generación de la Seguridad y con ello construir una sociedad más segura y que tenga confianza dentro de este ámbito. La educación en la Ciberseguridad nace de sensibilizar a todos, desde edades tempranas, pasando por jóvenes y adultos mayores, de los riesgos y las consecuencias de sus prácticas en Internet. Por ejemplo, Estados Unidos cuenta con el programa de educación "*National Initiative for Cybersecurity Education* (NICE)" desarrollado en el año 2012, promoviendo el avance de las personas en el tema de Ciberseguridad.

Sin embargo, existe una ausencia de un consenso general de que se debiese enseñar sobre Ciberseguridad en todo nivel, desde el nivel del ciudadano común hasta el nivel universitario. En este último debe haber un esfuerzo en el desarrollo curricular en este ámbito. La evolución de unos buenos programas de Ciberseguridad a nivel universitario es un cambio necesario en este frente. Existe una gran demanda de personas no solo en el país sino a nivel internacional bien calificadas en Ciberseguridad, es visto esto como una carrera para el futuro.

La universidad debe asumir el liderazgo para generar los espacios en el ámbito de la educación, desde cursos formales, cursos de extensión y la investigación científica. En este último, creando grupos de investigación que cuenten con recono-

cimiento por el valor de sus resultados. Esto puede habilitar la generación de conocimiento que pueda ser volcado a la sociedad y a las empresas.

Ahora bien, en la línea de lo anterior, es importante definir que del todo es lo más importante proteger y consecuentemente investigar sobre ello, en este caso la Infraestructura Crítica por el nivel de impacto que puede acarrear una interrupción en su funcionamiento. La Infraestructura Crítica como sistemas de generación y distribución de energía, redes de telecomunicaciones, control de oleoductos, entre otros, son el blanco de los ciberataques. El impacto y el costo de estas amenazas, así como la presión regulatoria para mitigarlas, han creado una agenda priorizada para los Estados.

La revisión de la madurez actual de la capacidad de resiliencia y los modelos de riesgo, destacan que, aunque muchos modelos existen, ninguno está específicamente diseñado para abordar el escenario de los operadores en Colombia, por el contrario, solo existen modelos parciales o de sectores específicos de la industria y todos están en un nivel general. La ausencia de un modelo de madurez de la capacidad de Ciberseguridad brinda una oportunidad para mayor investigación a expertos e investigadores de la industria de los modelos de madurez de capacidad de Ciberseguridad.

La resiliencia está surgiendo como la mejor estrategia para abordar el cambio y la incertidumbre en un conjunto cada vez mayor de sectores, escalas y plazos. Las partes interesadas y los expertos en la materia deben reflexionar sobre la integración entre la Ciberseguridad y los esfuerzos de desarrollo de la resiliencia en general. Los responsables de la Ciberseguridad deberían examinar cómo el pensamiento de resiliencia podría alterar los enfoques para gestionar los riesgos de forma explícita en el ciberespacio.

Igualmente, las empresas deben unir las técnicas de evaluación del riesgo junto con las técnicas financieras de análisis, para determinar la mejor manera de utilizar sus recursos y esfuerzo para aumentar los ingresos y disminuir los costos o las pérdidas. Sin embargo, pocas organizaciones tienen tales procesos de análisis para determinar el nivel y tipo de mecanismos de Ciberseguridad en los que invierten y mantener. Medir nivel óptimo no es sencillo, sin embargo, se puede conseguir una aproximación midiendo la posibilidad de ocurrencia de una brecha de seguridad versus el costo de si llegase a ocurrir. La resiliencia alimenta este modelo ya que, incorporándolo permite evaluar de manera fehaciente los tiempos de respuesta que se deben tener y los planes de recuperación para restaurar el sistema después de un compromiso de Seguridad. No existen métricas de rendimiento y evaluación que permitan determinar el nivel óptimo de inversión en Ciberseguridad, depende de factores relacionados con la eficiencia de la inversión.

La Ciberseguridad, que es el desafío común de todas las partes interesadas, debe aplicar el análisis de riesgos a cada uno de los vectores de amenaza. Si bien ninguno de nosotros puede saber exactamente cómo será el mundo futuro, creemos que es importante prestar atención a las tendencias clave de hoy que podrían dar forma a ese mundo y una de ellas, es todo lo relacionado con la Ciberseguridad y la ciberdefensa.

REFERENCIAS

A/69/112, Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional (Organización de las Naciones Unidas 30 de junio de 2014).

A/RES/66/24, Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional (Organización de las Naciones Unidas 2 de diciembre de 2011).

A/RES/71/28, Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional (Organización de las Naciones Unidas 5 de diciembre de 2016).

Aboso, G. (2006). *Cibercriminalidad y Derecho Penal, la información y los sistemas informáticos como nuevo paradigma del derecho penal, análisis doctrinario, jurisprudencial y de derecho comparado sobre los denominados "delitos informáticos"*

Acosta, O. P. y Martínez, J. J. (2017). Capacitación profesional y formación especializada en Ciberseguridad. *Cuadernos de Estrategia,* 1(185), 291-350.

AEPD; INCIBE. (s.f.). *Guía de privacidad y seguridad en Internet.* España: Agencia Española de Protección de Datos (AEPD); Instituto Nacional de Ciberseguridad (INCIBE).

AG/RES. 2004, Estrategia de Seguridad Cibernética (Organización de los Estados Americanos junio 8, 2004).

Alessandrini, A. (2016). *Ransomware Hostage Rescue Manual.* Clearwater, FL: KnowBe4.

Alonso García, J. (2015). *Derecho penal y redes sociales.* Madrid: Aranzadi.

Álvarez, E. (1 de mayo de 2013). *Hackers, crackers y hacktivistas: cinco episodios memorables.* Obtenido de Colombia Digital: https://colombiadigital.net/actualidad/noticias/item/4797-hackers-crackers-y-hacktivistas-cinco-episodios-memorables.html#a2

Amaral, A. C. (2014). La amenaza cibernética para la Seguridad y Defensa de Brasil. *Visión Conjunta, 6,*(10).

Antonopoulos, A. M. (2015). *Mastering Bitcoin.* Sebastopol: O'Reilly Media, Inc.

Arenilla Sáez, M. (marzo y abril de 2003). El Estado y la administración pública en la sociedad de la información. *Boletín ASTIC.*

Asobancaria. (2018). Asociación Bancaria y Entidades Financieras de Colombia – *Semana Económica, edición 1133.* 1-12

Assolini. F. (2018). Analista senior de seguridad en Kaspersky Lab. Resultados presentados en la *Octava Cumbre de Analistas de Seguridad para América Latina, Ciudad de Panamá,* véase en https://latam.kaspersky.com/blog/kaspersky-lab-registra-un-alza-de-60-en-ataques-ciberneticos-en-america-latina/13266/

Assurance, N. T. (2012). *Good Practice Guide Information Risk Management.* London.

Australian/Standards, N. Z.-S. (2009). Australia.

Ávila, R. (2016, septiembre 9). Amenazas cibernéticas y la vulnerabilidad de nuestro negocio. *Dinero.*

Barbier, E.A. (2002). *Contratación Bancaria, Tomo I, Consumidores y usuarios,* Buenos Aires: Editorial Astrea, 2° Edición, p. 42

Beck, U. (2008). *La sociedad del riesgo mundial. En busca de la seguridad perdida.* Barcelona: Paidós.

Bell, D. (1984). *Las Ciencias Sociales desde la Segunda Guerra Mundial.* Madrid: Alianza Editorial.

Benítez, P. (2013). ¿Democracia o democracia virtual? La Red y los movimientos de 2011. *Daimon Revista Internacional de Filosofía, 1,*(58), 33-50.

Beriain, J. (2005). *Modernidades en Disputa.* Barcelona: Anthropos.

Bericat Alastuey, E. (1996). La sociedad de la Información. Tecnología, cultura, Sociedad. Reis. *Revista española de investigaciones sociológicas,*76, 99-122.

BID y OEA (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? *Informe Ciberseguridad 2016.*

Bohórquez-Keeney, A. (2018). *Memorias Mesa Academia.* Bogotá D.C.: Escuela Superior de Guerra.

Broucek, V. & Turner, P. (2013). Technical, legal and ethical dilemmas: distinguishing risks arising from malware and cyber-attack tools in the 'cloud'—a forensic computing

perspective. *Journal of Computer Virology and Hacking Techniques, 9,*(1), 27-33.

Bundesamt für sicherheit in der informationstechnik. (2009). *Act to Strengthen the Security of Federal Information Technology.* Berlin: Bundesamt für sicherheit in der informationstechnik.

Bustos, J. L. (14 de mayo de 2013). *La importancia de la construcción de contextos en las investigaciones judiciales.* Jornadas Fiscalía General de la Nación Unidad de Análisis y Contextos (UNAC). Bogotá: Auditorio Compensar.

Buzan, B. & Hansen, L. (2009). *The Evolution of International Security Systems.* Cambridge: Cambridge University Press.

Cabaj, K., Gregorczyk, M. & Mazurczyk, W. (2018). Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics. *Computers & Electrical Engineering, 66*(1), 353-368.

Camargo Vega, J. J. Camargo Ortega, J. F. y Aguilar, L. J. (2015). Conociendo Big-Data. *Revista Facultad de Ingeniería, 24*(38), 63-77.

Carr, J. (2011). *Inside Cyber Warfare: Mapping the cyber underworld.* Sebastopol, CA: O'Reilly Media, Inc.

Carrasco, F. (2013). *Los 6 pasos que su organización debe seguir para confiar en Big Data.* América Latina. Recuperado de http://www. cioal.com/2013/07/31/los-6-pasos-que-suorganizacion-debe-seguir-para-confiar-en-bigdata

Casas Mínguez, F. (2016). *Sociedad del riesgo global.* (U. Universidad de Castilla -La Mancha, Ed.) Obtenido de Repo-

sitorio Universitario Institucional de Recursos Abiertos, RUIdeRA: http://hdl.handle.net/10578/12973

Casas Mínguez, F. (2016). *Sociedad del riesgo global.* (U. Universidad de Castilla -La Mancha, Ed.) Retrieved from Repositorio Universitario Institucional de Recursos Abiertos, RUIdeRA: http://hdl.handle.net/10578/12973

Castells, M. (2006). *La Sociedad Red: Una Visión Global.* Madrid: Alianza Editorial.

Castells, M. (1999, Mayo-Agosto). Globalización, sociedad y política en la era de la información. *Analisis Político(37),* 2-17.

CCOC. (2015). *Guía para la Identificación de Infraestructura Crítica Cibernética (ICC) de Colombia.* Bogotá D.C.: Comando General Fuerzas Militares.

Ceceña, A. E. (2008). *Hegemonía, emancipaciones y políticas de seguridad de América Latina.* Lima: Programa Democracia y Transformación Global.

Centro Cibernético Policial (2017). *Policía Nacional de Colombia, Dirección de investigación Criminal e Interpol.* Informe: Amenazas del cibercrimen en Colombia 2016 – 2017. pp. 1-2

Centro Global de Capacitación de Seguridad Cibernética en la Universidad de Oxford (2016).

Centrum, N. C. (2013). *National Cyber Security Strategy 2 From awareness to capability. National Coordinator for Security and Counterterrorism.*

Cernada Badía, R. (24 de octubre de 2012). Los actos de comunicación electrónicos como instrumento de una efectiva

tutela judicial (Trabajo de investigación presentado el 24 de octubre de 2012 en la U. Valencia, bajo la dirección de Lorenzo Cotino).

Chawki, M., Darwish, A., Khan, M. A. & Tyagi, S. (2015). *Cybercrime: introduction, motivation and methods.* In Cybercrime, Digital Forensics and Jurisdiction (pp. 3-23). Springer, Cham.

Chen, F., Deng, P., Wan, J., Zhang, D., Vasilakos, A. V. & Rong, X. (2015). Data Mining for the Internet of Things: Literature Review and Challenges. *International Journal of Distributed Sensor Networks, 11,*(8).

Chevallier, J. (2011). *El Estado posmoderno.* Bogotá: Universidad Externado de Colombia.

Christou, G. (2016). *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy.* Springer.

Clarke, R. & Knake, R. (2012). *Cyberwar: The Next Treat to National Secu-rity and What to Do About It.* Nova Iorque: Harper Collins.

Clinton, H. (2011). *Internet rights and wrongs: Choices & challenges in a networked world.* US State Department.

Coats, D. (2018). *Statement of the record, Worldwide threat assessment of the US Intelligence Community.* Office of the director of National Intelligence. United State of América.

Cohen, B., & Lee, I.-S. (1979, junio). A Catalog of Risks. *Health Physics, 36,*(6), 707-722.

Cohen, L. E., y Felson, M. (1979). *Social change and crime rate trends: A routine activity approach, en ASR, vol. 44,* núm. 4. pp. 588–608

Collier, Z. A., DiMase, D., Walters, S., Tehranipoor, M. M., Lambert, J. H., & Linkov, I. (2014). Cybersecurity standards: Managing risk and creating resilience. *Computer, 47,*(9), 70-76

Comisión de las Comunidades Europeas (2000). *Comunicación de la comisión al consejo, al parlamento europeo, al comité económico y social y al comité de las regiones.* Bruselas, 26.1.2001 COM (2000) 890 final. véase en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:ES:PDF

Comisión Europea, Comunicación de la Comisión al Consejo, al Parlamento Europeo y al Comité Económico y Social Europeo. (2008). *Hacia una Estrategia europea en materia de e-Justicia (Justicia en línea).* Recuperado de http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV%3Ajl0007.

Commerce, U. D. (08 de 08 de 2018). *National Institute of Standards and Technology.* Obtenido de National Institute of Standards and Technology: https://www.nist.gov/

Commonwealth of Australia. (2014). *Commonwealth Risk Management Policy.* Australia.

Computerworld.es. (2013). *El mercado del Big Data crecerá hasta los 32.400 millones de dólares en 2017.* Recuperado de http://www. computerworld.es/sociedad-de-la-información/ el-mercado-del-big-data-crecera-hasta-los-32400-millones-de-dolares-en-2017

Conpes 3701, Lineamientos de Política para Ciberseguridad y Ciberdefensa (Departamento Nacional de Planeación 14 de julio de 2011).

Conpes 3854, Política nacional de Seguridad Digital (Departamento Nacional de Planeación 11 de Abril de 2016). Obtenido de http://hdl.handle.net/11520/14856

Convenio de Budapest (2001). Consejo de Europa, p.2

Cornaglia, S., & Vercelli, A. (Junio de 2017). La Ciberdefensa y su regulación legal en Argentina (2006 - 2015). Urvio. *Revista Latinoamericana de Estudios de Seguridad(20),* 46-62.

Correa-Henao, G. J. y Yusta-Loyo, J. M. (2013). Seguridad energética y protección de infraestructuras críticas. *Lámpsakos, 1,*(10). doi: https://doi.org/10.21501/issn.2145-4086

Council of Europe (2001). *Serie de tratados europeos - no 185,* Convenio sobre la Ciberdelincuencia, Budapest, 23 XI.

Criado Grande, J. I. (2010). *Entre sueños utópicos y visiones pesimistas. Internet las TIC en la modernización de las Administraciones públicas,* Premio INAP, .

Croo, A. D. (2017). *Speech of Minister Alexander De Croo at the Cyber Security Conference 2017 of NATO/NIAS2017.* Belgica : Federal Public Service Foreign Affairs.

Cruz Lobato, L. (2017). La política brasileña de Ciberseguridad como estrategia de liderazgo regional. URVIO, *Revista Latinoamericana de Estudios de Seguridad 1,*(20), 16-30.

Danish Ministry of Finance. (2016). *A stronger and more secure digital denmark.* Denmark : Digital Strategy .

Dans, E. (2011. *Big Data, una pequeña introducción.* Recuperado de http://www.enriquedans. com/2011/10/big-data-una-pequenaintroduccion.html

Das, S. K., Kant, K. & Zhang, N. (2012). *Handbook on Securing Cyber-Physical Critical Infrastructure.* New York, NY: Morgan Kaufman Publishers.

De La Rosa, A. (2014b). Comunicación para la democracia: jóvenes y movimientos sociales. *Apuntes de Ciencia & Sociedad, 4,*(1), 118-124.

De La Rosa, A. (2014). *Social Media and Social Movements Around the World. Lessons and Theoretical Approaches.* En B. Pătruţ, & M. Pătruţ (Edits.), Social Media in Politics. Case Studies on the Political Power of Social Media (págs. 35-48). London: Springer.

De La Rosa, A. (2016). Movimientos sociales, redes sociales y recursos simbólicos. *Correspondencias & Análisis(6),* 47-60.

Decisión 587, Lineamientos de la Política de Seguridad Externa Común Andina (Consejo Andino de Ministros de Relaciones Exteriores 10 de julio de 2004).

Declaración sobre Seguridad en las Américas (2003). Conferencia especial sobre Seguridad, Organización de los Estados Americanos.

Delgado García, A. M. y Oliver Cuello, R. (2006). *Las tecnologías de la información y la comunicación en la Administración de Justicia.* Oñati: IVAP.

Delgado, R., Vargas, M., Vives, M., Luque, P., Lara, L. M. y Arias, R. L. (2005). *Estado del Arte: educación para el conocimiento social y político.* Bogotá: Pontificia Universidad Javeriana.

Deloitte (2016). *La Evolución de la Gestión de Ciber-Riesgos y Seguridad de la Información, Encuesta 2016 sobre Tendencias de Ciber-Riesgos y Seguridad de la Información en Latinoamérica.* Julio 2016. véase en: https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Deloitte%202016%20Cyber%20Risk%20%20Information%20Security%20Study%20-%20Latinoam%C3%A9rica%20-%20Resultados%20Generales%20vf%20(Per%C3%BA).pdf

Dennett, D. C. (2014). When HAL kills, who's to blame?: computer ethics. En: J. Nida-Rümelin & F. Battaglia (Eds.), *Rethinking responsibility in science and technology* (pp. 203-214). Pisa, Italia: Pisa University Press.

Departamento de Segurança da Informação e Comunicações. (2015). *Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal (2015-2018).* Brasília DF: Presidência da República.

Department of Defense. (2015). *The DoD Cyber Strategy,* Washington, D.C.: The Department of Defense.

Department, D. S. (2014). *Cyber Security Strategy for Defence.* Brusels: ACOS STRAT.

Department, D. S. (2014). *Cyber Security Strategy for Defence.* Brusels: ACOS STRAT.

Díez, L,(1999) *Derecho de Daños,* Madrid: Civitas

Directiva (UE) 2016/1148 del parlamento europeo y del consejo de 6 de julio de 2016. Relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

Directiva UE 1148, (Parlamento Europeo 06 de Julio de 2016). Relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

Directiva UE 1148, (Parlamento Europeo Julio 06, 2016). Relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión

Dunn, M. & Suter, M. (2012). The Art of CIIP Strategy: Tacking Stock of Content and Processes. En: J. López, R. Setola & S. D. Wolthusen (Eds.), Critical Infrastructure Protection (pp. 15-38). New York, NY: Springer.

Eidgenössisches Departement für Verteidigung,. (2012). *National strategy for Switzerland's,* Suiza: Eidgenössisches Departement für Verteidigung,.

Eijkman, Q. (2014). Digital Security Governance and Risk Anticipation: What About the Role of Security Officials in Privacy Protection? *International Political Sociology, 8*(1), 116-118. doi: https://doi.org/10.1111/ips.12046

Eisenberg, D. A., Linkov, I., Park, J., Bates, M., Fox-Lent, C. & Seager, T. (2014). Resilience metrics: lessons from military doctrines. *Solutions, 5*(5), 76-87.

El Tiempo. (2017, septiembre 27). A diario se registran 542.465 ataques informáticos en Colombia. *El Tiempo.*

El Tiempo. (27 de septiembre de 2017). A diario se registran 542.465 ataques informáticos en Colombia. *El Tiempo.*

Eom, J. h. (2014). Roles and Responsibilities of Cyber Intelligence for Cyber Operations in Cyberspace. *International Journal of Security and Its Applications, 8*(5), 323-332.

Escuela de Altos Estudios de la Defensa. (2014, junio). Estrategia de la Información y Seguridad en el Ciberespacio. *Documentos de seguridad y Defensa(60).* España: Ministerio de Defensa.

Escuela de Altos Estudios de la Defensa. (junio de 2014). Estrategia de la Información y Seguridad en el Ciberespacio. *Documentos de seguridad y Defensa(60).* España: Ministerio de Defensa.

ESET (2018). *Eset Security Report 2018.* Latinoamérica 2018. p. 6

ESET (2018). *Tendencias en Ciberseguridad 2018.* El costo de nuestro mundo conectado.

ESET. (2018). *Cybersecurity Trends 2018: The Cost Of Our Connected World.* Bratislava: Eset.

Espugla Trenc, J. (2006). Dimensiones sociales de los riesgos tecnológicos: el caso de las antenas de telefonía móvil. *Papers: revista de sociologia (82),* 79-95. doi:10.5565/rev/papers/v82n0.2050

Estado-Maior Conjunto das Forças Armadas. (2014). *Doutrina Militar de Defesa Cibernética.* Brasília DF: Ministério da Defesa.

Fachkha, C. & Debbabi, M. (2016). Darknet as a Source of Cyber Intelligence: Survey, Taxonomy, and Characterization. *Communications Surveys & Tutorials, 18*(2), 1197-1227.

Felson, M. Routine activities and crime prevention, Studies on Crime and Crime prevention: *Annual Review,* 1 pp. 30 y ss.

Fernández, M. A., & Sáez Domingo, D. (2015). *Del Internet de las Cosas a los Sistemas Ciber-Físicos.* Valencia: Observatorio Tecnológico; Instituto Tecnológico de Informática.

Fiscalía General de la Nación, (2015). Directiva 002 de 2015, por medio de la cual se amplía y modifica la Directiva 01 de 2012, se desarrolla el alcance de los criterios de priorización de situaciones y casos, y se establecen lineamientos para la planificación y gestión estratégica de la investigación penal en la Fiscalía General de la Nación. Recuperado de http://www.fiscalia.gov.co/colombia/priorizacion/normativa/

Fiscalía General de la Nación (2016a). *Visión.* Bogotá: Fiscalía General de la Nación.

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S. & combs, B. (1978). How safe is safe enough? A psychometric study of actitudes towards technological risks and benefits. *Policy Sciences(9),* 127-152.

Foro Económico Mundial (2018) *Informe de riesgos mundiales 2018,* 13.a edición. Ginebra p. 6.

Foro Económico Mundial. (2016). Economía digital y seguridad en América Latina y el Caribe. En: O. Ciberseguridad (Ed.), *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?* (pp. 25-30). Washington, D.C.: Banco Interamericano de Desarrollo.

Foro Económico Mundial. (2017). *Informe de riesgos mundiales.* Ginebra: World Economic Forum.

Fundación Innovación Bankinter. (2011). *El Internet de las Cosas en un mundo conectado de objetos inteligentes.* Madrid: Fundación de la Innovación Bankinter; Accenture.

Gaitán, A. (2012). *El ciberespacio: un nuevo teatro de batalla para los conflictos armados del siglo XXI.* Bogotá D.C.: Esdegue.

Gamero Casado, E. (2012). El objeto de la Ley 18/2011 y su posición entre las normas relativas a las tecnologías de la información. En Gamero Casado, E. y Valero Torrijos, J., coordinadores. *Las tecnologías de la información y la comunicación en la Administración de Justicia.* Análisis sistemático de la Ley 18/2011, de 5 de julio (p. 45-88). Cizur Menor, Navarra: Thomson Reuters-Aranzadi.

García Font, V., Garrigues, C. y Rifá Pous, H. (2014). Seguridad en smart cities e infraestructuras críticas. *Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información.* 221-226.

Garriga, A. (2016). *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua.* Madrid: Editorial DYKINSON S.I.

Gascó Hernández, M. (2001). *Una aproximación a la definición de políticas de inserción en la sociedad de la información.* VI Conferencia CLAD.

Gascón Inchausti, F. (2010). La e-Justicia en la Unión Europea: balance de situación y planes para el futuro (en diciembre de 2009). En Senés Montilla, Carmen [coord.]. *Presente y futuro de la e-Justicia en España y la Unión Europea* (p. 84-85). Cizur Menor (Navarra): Aranzadi.

Genge, B., Kiss, I. y Haller, P. (2015). A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. *International Journal of Critical Infrastructure Protection, 10*(1), 3-17.

Giddens, A. (1990). *Las Consecuencias de la Modernidad.* España: Alianza Editorial.

Giudici, D. E. (2013). *Lineamientos para la seguridad cibernética en Teatro de Operaciones.* Buenos Aires: Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Gobierno de Argentina. (2018). *Normativa - Ciberseguridad.* Recuperado el 21 de Febrero, 2018, de https://www.argentina.gob.ar/normativa-ciberseguridad

Gobierno de Chile. (2017). *Política Nacional de Ciberseguridad.* Santiago: Gobierno de Chile.

Gomes de Assis, C. (Junio de 2017). The new era of information as power and the field of Cyber Intelligence. Urvio. *Revista Latinoamericana de Estudios de Seguridad(20),* 94-109.

González, I. (9 de Febrero de 2018). *Usuarios de Internet y redes sociales en el mundo en 2018.* Obtenido de ILIFEBELT Times: https://ilifebelt.com/usuarios-Internet-redes-sociales-mundo-2018/2018/02/

H.R. 4036, Active Cyber Defense Certainty Act (115th Congress 1 de noviembre de 2017).

Hansson, S. O. (2000). *Seven Myths of Risk. Stockholm thirty years on. Progress achieved and challenges aheadin international environmental co-operation.* Suiza: Ministerio de Medio Ambiente.

Haufler, V. (2006). International Governance and the Private Sector. En C. May (Ed.), *Global Corporate Power. International Political Economy Yearbook* (págs. 80-103). Boulder: Lynne Rienner Publishers.

Hinestroza Vélez, J. P. (14 de mayo de 2013). *La importancia de la construcción de contextos en las investigaciones judiciales.* Fiscalía General de la Nación Unidad de Análisis y Contextos (UNAC). Bogotá: Auditorio Compensar.

Hohenemser, C., Kates, R., & Slovic, P. (1983). The nature of technological hazard. *Science, 220*(4595), 378-384.

Housen-Couriel, D. (2017). *National Cyber Security Organisation:* ISRAEL. Tallin: CCDCOE.

Huang, X., Craig, P., Lin, H. & Yan, Z. (2016). SecIoT: a security framework for the Internet of Things. *Security and Communication Networks, 9*(16), 3083-3094.

ICIC. (2018). *¿Qué hacemos?* Recuperado el 21 de Febrero, 2018, de http://www.icic.gob.ar/

Icontec. (08 de 08 de 2018). *ICONTEC.* Obtenido de ICONTEC: http://www.icontec.org/Paginas/Home.aspx

Icontec. (2018, 08 08). *ICONTEC.* Retrieved from ICONTEC: http://www.icontec.org/Paginas/Home.aspx

ITU (2014), *Global Cybersecurity Index,* www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

Jiménez, L. M., Pacagüi, A. L. & Rodríguez, A. M. (2014). Training Education Application to Technologies of the Information and Communication (TIC) and Digital Information Security. En: W. Briceño & J. A. Parra (Eds.), *Colección de Investigaciones en Innovación y Apropiación de las Tecnologías de la Información y las Comunicaciones.* Bucaramanga: Universidad Autónoma de Bucaramanga.

Kenner, A. (2014). Designing digital infrastructure: Four Considerations for Scholarly Publishing Projects. *Cultural Anthropology,* 29(2), 264-287.

Kepchar, K. J. (2016). Cybersecurity & critical infrastructure – are we missing the obvious? *INSIGHT, 19*(4), 54-58.

Kernaghan, K. (2014). Digital dilemmas: Values, ethics and information technology. *Canadian Public Administration, 57*(2), 295-317.

Kittichaisaree, K. (2017). *Public International Law of Cyberspace* (Vol. 32). Springer.

Klare, M. T. (2003). *Guerras por los recursos: el futuro escenario del conflicto global.* Ediciones Urano: México.

Klinke, A., & Renn, O. (2001). Precautionary principle and discursive strategies: Classifyng and managing risks. *Journal of Risk Research(4),* 159-173.

Klinke, A., & Renn, O. (2002). A new approach to risk evaluation and management: risk-based, precaution-based, and discourse-based strategies. *Risk Analysis(22),* 1071-1094.

Kosseff, J. (2017). *Cybersecurity Law. Hoboken,* NJ: John Wiley & Sons, Inc.

Lapuente Sastre, G. (2006). *Presupuestos epistemológicos del principio precaución.* I Congreso Iberoamericano de Ciencia, Tecnología, Sociedad e Innovación CTS+I (págs. 1-10). México: Organización de Estados Iberoamericanos para la Educación la Ciencia y la Cultura; Agencia Española de Cooperación Internacional; Universidad Nacional Autónoma de México.

Lewis, J. A. (2016). *Experiencias avanzadas en políticas y prácticas de Ciberseguridad.* Washington, D.C.: Banco Interamericano de Desarrollo.

Ley 1273, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comu (Congreso de Colombia 5 de enero de 2009).

Ley 1288, Por medio del cual se expiden normas para fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con su misión constitucional y legal, y se dictan otras disposiciones (Congreso de la Republica de Colombia 5 de Marzo de 2009).

Lopes, G. (20 de febrero de 2013). *Reflexos da digitalização da Guerra na política internacional do XXI: uma análise exploratória da securitização do ciberespaço nos Estados Unidos, Brasil e Canadá.* Tesis de Maestría en Ciencia Política. Brasil: Universidade Federal de Pernambuco.

Losavio, M. M., Chow, K. P., Koltay, A. & James, J. (2018). *The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security. Security and Privacy, e23.*

Lu, R., Zhu, H., Liu, X., Liu, J. K. & Shao, J. (2014). Toward efficient and privacy-preserving computing in big data era. *IEEE Network, 28*(4).

Luhmann, N. (2007). *La sociedad de la sociedad.* México: Heder.

Luis García, L. C. (2015). *Estudio del impacto técnico y económico de la transición de Internet al Internet de las Cosas (IoT) para el caso colombiano.* Tesis de investigación presentada como requisito parcial para optar al título de Magister en Ingeniería de Telecomunicaciones. Bogotá: Universidad Nacional de Colombia.

Maira, L. (2005). La Gobernabilidad y la globalización. En R. Torrent Macau, A. Millet Abbad, & A. Arce Suárez (Edits.), *Diálogo sobre gobernabilidad, globalización y desarrollo.* Barcelona: Universidad de Barcelona.

Makili-Aliyev, K. (2013). *Cyber-Security Objective: Azerbaijan In The Digitalized World.* Baku: Center For Strategic Studies.

Mariscal, S. A. (Septiembre de 2016). *Impacto de las Tic en las Relaciones de Poder y en la Emergencia de Nuevos Actores Internacionales.* Tesis Doctoral en Relaciones Internacionales e Integración Europea. Barcelona: Universidad Autónoma de Barcelona.

Martín Del Barrio, J. (19 de febrero de 2018). El secretario general de la ONU dice que hay "ciberguerra entre Estados". *El País.*

Martín Del Barrio, J. (2018, febrero 19). El secretario general de la ONU dice que hay "ciberguerra entre Estados". *El País.*

Martin Rodrigo, T. (2001). Proyecto para una administración electrónica en España. *Revista del CLAD Reforma y Democracia (20),* 199.

Martín, E. (2016). Los retos de la ciberinteligencia. Cuadernos de la Guardia Civil, 1(53), 53-67.

Martín, E. (2017). Dark Web y Deep Web como fuentes de ciberinteligencia utilizando minería de datos. *Cuadernos de la Guardia Civil, 1*(54), 74-93.

Martínez Osorio, D. (14 de mayo de 2013). La importancia de la construcción de contextos en las investigaciones judiciales. En *Actas de Fiscalía General de la Nación, Unidad de Análisis y Contextos (UNAC).* Bogotá: Auditorio Compensar.

Martínez, J. M., Mejía, J., Muñoz, M., & García, Y. M. (2017, Mayo-Octubre). *La Seguridad en Internet de las Cosas: Analizando el Tráfico de Información en Aplicaciones para iOS.*

Martínez, Ó. G. & Hernández, J. M. (2017). Ransomware Wanna Cry, ¿qué es y cómo proteger nuestros equipos? *Unversitaria, 1*(1).

México. (2017). *Estrategia Nacional de Ciberseguridad.* México DF: México.

Minárik, T. (2016). *National Cyber Security Organisation: Czech Republic.* Tallinn: NATO.

Ministry of Economic Affairs and Communication. (2014). *Cyber Security Strategy.* Tallin: Ministry of Economic Affairs and Communication.

Ministry of Interior of Republika Srpska. (2017). *Cybercrime policies/strategies. Bosnia and Herzegovina:* Bosnia and Herzegovina.

Ministry of Transport and Communications. (2016). *Finland to become the world leader in corporate information security.* Helsinki: Ministry of Transport and Communications.

Minsky, M. (1988). *The Society of Mind.* New York: Simon & Schust.

Mintic. (2018, junio 10). *Ciberseguridad.* Retrieved from Investigación, Desarrollo e Innovación: https://www.mintic.gov.co/portal/604/articles-6120_recurso_1.png

Mintic. (10 de junio de 2018). *Ciberseguridad.* Obtenido de Investigación, Desarrollo e Innovación: https://www.mintic.gov.co/portal/604/articles-6120_recurso_1.png

Mintic. (2014). *Agenda Estratégica de innovación: Ciberseguridad.* Bogotá: Ministerio de Tecnologías de la Información y las Comunicaciones, Cintel.

Mintic. (2014). *Agenda Estratégica de innovación: Ciberseguridad.* Bogotá: Ministerio de Tecnologías de la Información y las Comunicaciones, Cintel.

Miró, F. (2012). *El cibercrimen, Fenomenología y criminología de la delincuencia en el ciberespacio.* Madrid, Marcial Pons. p. 13

Moffa, T. (1 de 11 de 2012). *Canada's national cryptologic agency.* Obtenido de Communications Security Establishment: https://www.cse-cst.gc.ca/en/publication/itsg-33

Moffa, T. (2012, 11 1). *Canada's national cryptologic agency.* Retrieved from Communications Security Establishment: https://www.cse-cst.gc.ca/en/publication/itsg-33

Molano, A. (1 de Octubre de 2014). *Internet de las cosas: concepto y ecosistema.* Obtenido de Colombia Digital: https://colombiadigital.net/actualidad/articulos-informativos/item/7821-Internet-de-las-cosas-concepto-y-ecosistema.html

Moncada, E. (11-13 de Noviembre de 2015). *Seguridad hídrica en los sistemas de irrigación.* Mendoza, Argentina.

Mosca, L., & Porta, D. (2009). *Democracy in Social Movements.* Chippenham: Palgrave Mcmillan.

Muñoz, J. M. (2005). Los cambios de la era digital en las sociedades de los medios de masas, su incidencia en la esfera de la publicidad y el problema de la corporalidad. *Thémata (35),* 559-564.

NCSI, "*NCSI Methodology,*" http://ncsi.ega.ee/methodology (1.0) and http://ncsi.ega.ee/ncsi-methodology-2-0-launched/ (2.0).

Neiva Santos, R. (2009). *Petrobras en la política exterior del gobierno de Lula: una mirada desde la Economía Política internacional,* (tesis de maestría). Buenos Aires: Universidad de San Andrés; Universidad de Barcelona.

Newhouse, W., Keith, S., Scribner, B. & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.* Washington D.C.: U.S. Department of Commerce.

Nuix, Defending Data: Turning Cybersecurity Inside Out With Corporate Leadership Perspectives on Reshaping Our Information Protection Practices, 2015, pp. 6, 10

OEA. (2018). *Comité Interamericano contra el Terrorismo.* Obtenido de Organización de los Estados Americanos: http://www.oas.org/es/sms/cicte/default.asp

OCDE. (2016). *Broadband Policies for Latin America and the Caribbean: A Digital Economy Toolkit.* París: Organización para la Cooperación y el Desarrollo Económicos.

OCDE (2015). http://www.oecd.org/Internet/broadband/lac-digital-toolkit/es/Site,Container/Politicas,de,Banda,Ancha,para,America,Latina,y,el,Caribe,Un,Manual,para,la,Economia,Digital/toolkit-text-chapter14es.htm

OCDE. (2015). *Digital Security Risk Management for Economic and Social Prosperity.* Francia: Organización para la Cooperación y el Desarrollo Económicos.

OCDE. (2015b). *Principales objetivos de las políticas para la región LAC.* Obtenido de Políticas de Banda Ancha para América Latina y el Caribe: Un Manual para la Economía Digital: http://www.oecd.org/Internet/broadband/lac-digital-toolkit/es/toolkit-text-chapter14es.htm

OCDE. (2003). *Emerging Risks in the 21st Century. An Agenda for Action.* París: Organización para la Cooperación y el Desarrollo Económicos.

Olcott, D., Carrera, X., Gallardo, E. E. & González, J. (2015). Ética y Educación en la era digital: perspectivas globales y estrategias para la transformación local en Cataluña. *RUSC. Universities and Knowledge Society Journal, 12(2),* 59-72. doi: http://dx.doi.org/10.7238/rusc.v12i2.2455

Olivé, L. (julio de 2004). La democratización de la ciencia desde la perspectiva de la ética. En J. A. López Cerezo, *La democratización de la ciencia* (Cátedra Miguel Sánchez-Mazas) (págs. 159-175). Tolosa etorbidea: Erein Argitaletxea.

Organisation For Economic Co-Operation And Development. (2015). *Digital Security Risk Management.* Paris, Paris, Francia: OECD.

Organización de los Estados Americanos, MinTIC y BID (2017). *Impacto de los incidentes de Seguridad Digital en Colombia 2017.* p. 14

Orozco, L. (2016). Los actores subnacionales en la nueva fase del proceso de globalización. *Revista de Comunicación(15),* 183-197.

Ortiz Pradillo, J. C. (2013). La investigación del delito en la era digital Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación. *Estudios de progreso, Fundación Alternativas, 74.*

Otniel, D. (2015). *Risk Management In Future Romanian E-Government 2.0 Projects. Studia Universitatis.*Vasile Goldis" Arad – Economics Series, 11-22.

Pathak, P. B. & Nanded, Y. M. (2016). A Dangerous Trend of Cybercrime: Ransomware Growing Challenge. *International Journal of Advanced Research in Computer Engineering & Technology, 5*(2).

Pawlak, P., & Wendling, C. (2013). Trends in cyberspace: ¿can governments keep up? *Environment Systems and Decisions, 33*(4), 536-543.

Pérez, A, (1996). *Ensayos de informática jurídica.* México: Fontamara, p. 18.

Pernik, P. & Tuohy, E. (2016). *Interagency Cooperation on Cyber Security: The Estonian Model.* Brussel: NATO.

Piccirilli, D. (2016). *Protocolos a aplicar en la forensia informática en el marco de las nuevas tecnologías* (pericia – forensia y cibercrimen). UNLP, La Plata.

Planeación, D. N. (08 de 08 de 2018). *Departamento Nacional de Planeación.* Obtenido de Departamento Nacional de Planeación: https://www.dnp.gov.co/CONPES/paginas/Conpes.aspx

Policía Nacional de Colombia; Ministerio de Defesa Nacional. (2018). Servicios. Obtenido de Centro Cibernético Policial: https://caivirtual.policia.gov.co/

Polícia Nacional. (2017b). *Balance cibercrimen en Colombia.* Colombia: Policía Nacional, Dirección de Investigación Criminal, Interpol.

Policía Nacional. (2017). *Amenazas del cibercrimen en Colombia 2016-2017.* Bogotá: Policía Nacional, Dirección de Investigación Criminal; Interpol.

Policía Nacional. (2017b). *Balance cibercrimen en Colombia. Colombia.* Policía Nacional, Dirección de Investigación Criminal, Interpol.

Pons Gamón, V. (Junio de 2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y Ciberseguridad. Urvio. *Revista Latinoamericana de Estudios de Seguridad(20),* 80-93.

Portafolio. (16 de Octubre de 2017). Colombia debe estar abierta a los cambios de la cuarta revolución industrial. *Portafolio.*

Portafolio. (2011, mayo 27). G8 promueve desarrollo de Internet en el mundo. *Portafolio.*

Portafolio. (27 de mayo de 2011). G8 promueve desarrollo de Internet en el mundo. *Portafolio.*

Rameli, A. (14 de mayo de 2013). *La importancia de la construcción de contextos en las investigaciones judiciales.* Fiscalía General de la Nación Unidad de Análisis y Contextos (UNAC). Bogotá: Auditorio Compensar.

Rashi Foundation. (2018). *Magshimim Program* Recuperado el 22 de Febrero, 2018, de https://www.rashi.org.il/magshimim-cyber-program

Rayón, M. C. & Gómez, J. a. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. *Anuario Jurídico y Económico Escurialense, 1(XLVII),* 209-234.

Reed, M. (14 de mayo de 2013). Oficina de la Alta Comisionada de Naciones Unidas para los Derechos Humanos (OACNUDH). La importancia de la construcción de contextos en las investigaciones judiciales. *Fiscalía General de la*

Nación Unidad de Análisis y Contextos (UNAC). Bogotá: Auditorio Compensar.

Renn, O. (2005). *White paper on risk governance: Towards an intergrative approach.* Genova: International Risk Governance Council.

Resilience, D. A National Imperative. (2012). *Committee on Increasing National Resilience to Hazards and Disasters.* NAC. Washington, 216.

Revista Semana. (2017, diciembre 28). El cibercrimen en 2017: la amenaza crece sobre Colombia. *Revista Semana.*

Revista Semana. (02 de Diciembre de 2006). La Guerra virtual. *Revista Semana.*

Revista Semana. (2017, Octubre 16). Colombia debe estar abierta a los cambios de la cuarta revolución industrial. *Portafolio.*

Revista Semana. (28 de diciembre de 2017). El cibercrimen en 2017: la amenaza crece sobre Colombia. *Revista Semana.*

Reyes Beltrán, P. (2017). *Derecho y globalización. Transformaciones del Estado contemporáneo.* Bogotá: Universidad Nacional de Colombia.

Rivera Berrío, J. G. (2009). Un modelo de gobernanza para gestionar el riesgo. *Trilogía. Ciencia, Tecnología, Sociedad(1),* 1-17.

Rivera Méndez, R. G. (2010). *Gobernanza Democrática. Concepto y Perspectivas.* Bolivia: Unidad de Gobernabilidad y Gobernanza; PADEP GTZ.

Robert Vargas, Rolando P. Reyes & Recalde, L. (2017). Ciberdefensa y Ciberseguridad, más allá del mundo virtual modelo ecuatoriano de gobernanza en Ciberdefensa. *Latinoamericana de Estudios de Seguridad, 1*(20), 31-45.

Roberto, B., & Montanari, L. (2015). *Italian National Cyber Security Framework. Int'l Conf. Security and Management* (pp. 168-174). Italia: ACM Digital Library .

Roel Pineda, V. (1998). *La Tercera Revolución Industrial y la Era del Conocimiento.* Lima: Universidad Nacional Mayor de San Marcos.

Roman, R., Zhou, J. & López, J. (2013). On the features and challenges of security and privacy in distributed Internet of things. *Computer Networks, 57*(10), 2266-2279.

Roth, A. N. (2002). *Políticas Públicas: Formulación, implementación y evaluación.* Bogotá D.C.: Ediciones Aurora.

Russom, P. (2012). *Big Data Analytics, TDWI.* The Data Warehousing Institute.

s.a. (2015). *Korea Internet White Paper.* Seoul: Korea Internet & Security Agency.

Sádaba, I. (2002). *Nuevas Tecnologías y política: Acción colectiva y movimientos sociales en la sociedad de la información.* Obtenido de Fundación Uned: https://www2.uned.es/ntedu/espanol/master/segundo/modulos/poder-y-control/medios_disponemos_sadaba.pdf

Saiz, E. (13 de marzo de 2013). Los ciberataques sustituyen al terrorismo como primera amenaza para EE UU. *El País.* Recuperado de http://internacional.elpais.com/internacional/2013/03/13/actualidad/1363187707_199021.html.

Salgado, M. (2014). *Oracle apuesta por Big Data con tecnología y proyectos.* Recuperado de http://www.computerworld.es/big-data/oracle-apuesta-por-big-data-con-tecnologia-yproyecto

Sánchez, N. (2018). *Análisis de las tendencias del comportamiento de ransomware en sistemas operativos android.* UNAD, Bogotá D.C.

Sancho, C. (2017). Ciberseguridad. Presentación del dossier. URVIO - *Revista Latinoamericana de Estudios de Seguridad, 8*(10), 8-15.

Sassen, S. (2015). *Una sociología de la globalización.* Buenos Aires: Katz Editores.

Saurí, D. (1995). *Geografia y riesgos tecnológicos.* Doc. Ad. Geogr, 147-158.

Schettini, P., & Cortazo, I. (2015). *Análisis de datos cualitativos en la investigación social. Procedimientos y herramientas para la interpretación de información cualitativa.* La Plata: Universidad Nacional de La Plata. Obtenido de http://stel.ub.edu/sites/default/files/agenda/documents/analisis_de_datos_cualitativos_1.pdf

Searchstorage.techtarget.com. (2012). *Examining HDFS and NameNode in Hadoop architecture.* Recuperado de http://searchstorage.techtarget. com/video/Examining-HDFS-and-NameNodein-Hadoop-architecture

Secretaría de Gobierno Digital. (2017). *Política Nacional de Ciberseguridad.* Lima: Presidencia del Consejo de Ministros.

Segura, A. (2017). Ciberseguridad y derecho internacional. *Revista Española de Derecho Internacional, 69*(2), 291-300.

Service, G. D. (2017). *Management of Risk in Government. A framework for boards and examples of what has worked in practice.* London.

Shackelford, S. J. & Andres, R. B. (2010). *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem.* Geo. J. Int'l L., 42, 971.

Shackelford, S., Schneier, B., Sulmeyer, M., Boustead, A., Buchanan, B., Craig, A., . . . Zhanna, J. (2017). *Making Democracy Harder to Hack: Should Elections Be Classified as 'Critical Infrastructure?'.* University of Michigan Journal of Law Reform, Kelley School of Business Research Paper No. 16-75.

Shen, L. (2013). NIST Cybersecurity Framework: Overview and Potential Impacts, *The. SciTech Law., 10,* 16.

Singer, P. W. & Friedman, A. (2014). *Cybersecurity and Cyberwar: What everybody needs to know.* New York: Oxford University Press.

Slovic, P. (1990). Perceptions of Risk: Reflections on the Psychometric Paradigm. En D. Golding, & S. Krimsky (Edits.), *Theories of Risk* (págs. 1-71). New York : Praeger.

Standardization, I. O. (08 de 08 de 2018). *International Organization for Standardization.* Obtenido de International Organization for Standardization: https://www.iso.org/home.html

Starr, C. (1969, Septiembre 19). Social Benefit versus Techonological Risck. *Science, 165*(3899), 1232-1238. doi:10.1126/science.165.3899.1232

Stirling, A. (2009). Ciencia, precaución y evaluación de riesgos:

hacia un debate más constructivo. En C. Moreno Castro, B. De Marchi, M. Gallent Marc, C. Polino, M. E. Fazio, M. Cámara Hurtado, . . . a. Stirling, & C. Moreno Castro (Ed.), *Comunicar los riesgos. Ciencia y tecnología en la sociedad de la información* (págs. 327-346). Madrid: OEI-Biblioteca Nueva.

Streżyńska, A. (2016). *Directions of Strategic Actions of the Minister of Digital Affairs in the field of computerization of public services.* Varsovia: Ministry of Digital Affairs.

Sula, C. A. (2016). Research Ethics in an Age of Big Data. *Bulletin of the Association for Information Science and Technology, 42*(2), 17-21. doi: https://doi.org/10.1002/bul2.2016.1720420207

Svein Ølnes, J. U. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Elsevier,* 355-364.

Tabernero, M. d., Moyano, M., & Trujillo, H. (17-19 de septiembre de 2014). *El modelo de Klinke y Renn en la evaluación y Gestión del Riesgo de radicalización y terrorismo.* Congreso Internacional de Estudios Militares. Granada, España: Centro Mixto Universidad de Granada; Mando de Adiestramiento y Doctrina del Ejército de Tierra (MADOC); Fundación General Universidad de Granada.

Tascón, M. (2013). *Dossier Big Data. TELOS Cuadernos de Comunicación e Innovación,* junio-septiembre, 46-96.

Taylor, S. J., & Bogdan, R. (1994). *Introducción a los métodos cualitativos de investigación.* Barcelona: Paidós.

Technology, N. I. (2017). *Framework for Improving Critical Infrastructure Cybersecurity.* Gaithersburg: NIST.

Tejero, A. (2017). *Metodología de análisis de riesgos para la mejora de la seguridad del Internet de las Cosas. Caso Smartwatch.* Madrid: Universidad Politécnica de Madrid.

The Ministry of Foreign Affairs of the Russian Federation. (2016). *Doctrine of Information Security of the Russian Federation.* Moscú.

Thomas, J. E. (2018). Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks. *International Journal of Business Management, 12*(3), 1-23.

Torres, J. (20 de Octubre de 2014). *¿Qué es y cómo funciona el Internet de las cosas?* Obtenido de Hipertextual: https://hipertextual.com/archivo/2014/10/Internet-cosas/

Torres-Soriano, M. R. (2017). Hackeando la democracia: operaciones de influencia en el ciberespacio. *Boletín I.E.E.E., 1*(6), 826-839.

Trigo, F. A. y López, M. J. (2004) Tratado de la responsabilidad civil. Tomo IV. Buenos Aires: La Ley. p. 931.

Unesco. (2005). *Hacia las sociedades del conocimiento.* París: Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura.

Unesco. (2017). *Cumbre Mundial sobre la Sociedad de la Información (CMSI).* Obtenido de Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura: http://www.unesco.org/new/es/communication-and-information/resources/multimedia/photo-galleries/world-summit-on-the-information-society-wsis/

UNODA. (2018). *Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional.* Obtenido de Oficina de Asuntos de Desarme de las Naciones Unidas: https://www.un.org/disarmament/es/los-avances-en-la-informatizacion-y-las-telecomunicaciones-en-el-contexto-de-la-seguridad-internacional/

Uribe Saavedra, A., Rialp Criado, J., & Llonch Andreu, J. (2013, julio-diciembre). EL uso de las redes sociales digitales como herramienta de marketing en el desempeño empresarial. *Cuadernos de Administración, 26*(47), 205-231.

Vaks, T. (2017). Annual Cyber Security Assessment. Tallinn.

Valero Torrijos, J. (2007). La nueva regulación legal del uso de las tecnologías de la información y las comunicaciones en el ámbito administrativo: ¿el viaje hacia un nuevo modelo de Administración, electrónica? *Revista Catalana de Derecho Público 35.*

Valle, V. (2003). *Derechos humanos, acceso a la información y seguridad humana.* Seminario Internacional Seguridad Internacional contemporánea: consecuencias para la seguridad humana en América Latina (págs. 46-52). Chile: Flacso -Chile, Unesco.

Valls, M. (16 de Octubre de 2015). *The French National Digital Security Strategy: Meeting The Security Challenges Of The Digital World.* Paris, Paris, Francia.

Valls, M. (2015, Octubre 16). *The French National Digital Security Strategy: meeting the security challenges of the digital world.* Paris, Paris, Francia.

Vargas Guillén, G. (1999). *Las líneas de investigación: de la posibilidad a la necesidad, en el desarrollo de líneas de investigación a partir de la relación docencia e investigación en la Universidad Pedagógica Nacional.* Bogotá: Universidad Pedagógica Nacional

Vargas Silva, L. E. (14 de mayo de 2013). *La importancia de la construcción de contextos en las investigaciones judiciales.* Jornadas Fiscalía General de la Nación Unidad de Análisis y Contextos (UNAC). La importancia de la construcción de contextos en las investigaciones judiciales. Bogotá: Auditorio Compensar.

Vicente, L. (2004, julio-agosto). ¿Movimientos sociales en la red? Los hacktivistas. *El Cotidiano, 20*(126), 1-8.

WEF (2018), *Cyber Resilience Playbook for Public-Private Collaboration,* pp. 33-36, https://www.weforum.org/reports/cyber-resilienceplaybook-for-public-private-collaboration

Wendt, A. (1992). Anarchy is what states make of it: the social construction of power politics. *International organization, 46*(2), 391-425

Wills, M. E. (14 de mayo de 2013). *La importancia de la construcción de contextos en las investigaciones judiciales.* Fiscalía General de la Nación Unidad de Análisis y Contextos (UNAC). Bogotá: Auditorio Compensar.

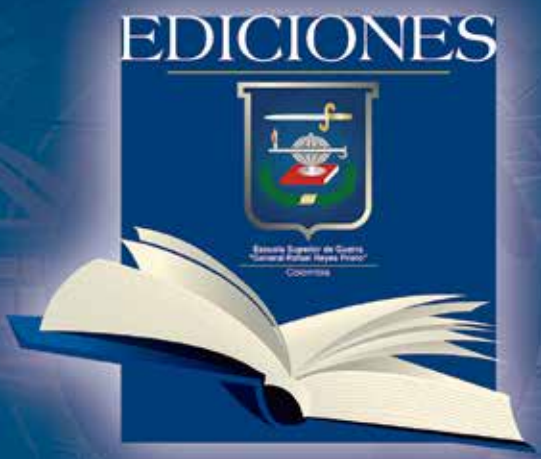
WSIS, Geneva 2003 - Tunis 2005, "Tunis Commitment," 18 November 2005, www.itu.int/net/wsis/docs2/tunis/off/7.html

Wynne, B. (1998). May the Sheep Safely Graze? A Reflexive View of the Expert–Lay Knowledge Divide. En S. Lash, B. Szerszynski, & B. Wynne, Risk, *Environment and Modernity: Towards a New Ecology* (págs. 44-83). Londres: Sage.

Yasunaga, M. (2017). Las nuevas tecnologías de votación: ¿una puerta abierta a la injerencia externa? *Boletín I.E.E.E., 1*(5), 703-716.

.

.



EsdegCol

@EsdegCol

Escuela Superior de Guerra

EsdegCol

issuu
esdeguecol

ESCUELA SUPERIOR DE GUERRA
“General Rafael Reyes Prieto”
#ESDEG
Carrera 11 No. 102-50
Conmutador: 620 4066
Bogotá, Colombia
www.esdegue.edu.co

ISO 9001:2015
BUREAU VERITAS
Certification