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

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.

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"

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.

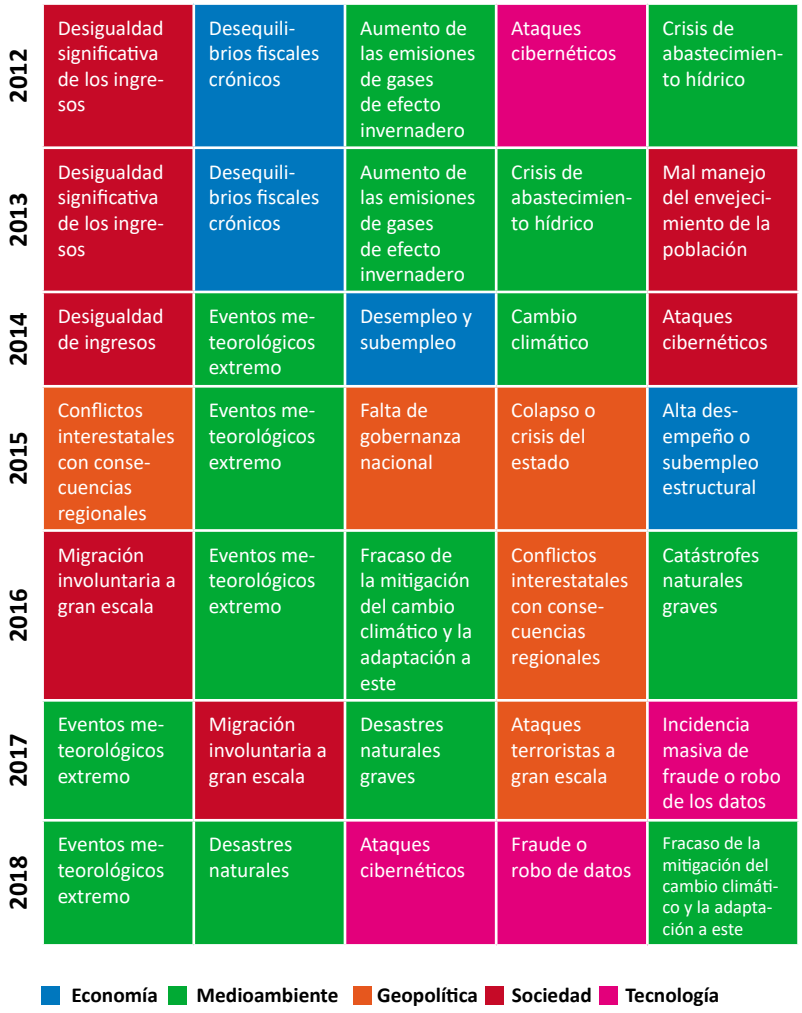


Ilustración 6. Los cinco riesgos globales en términos de probabilidad por el Foro Económico Mundial (2018).

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.

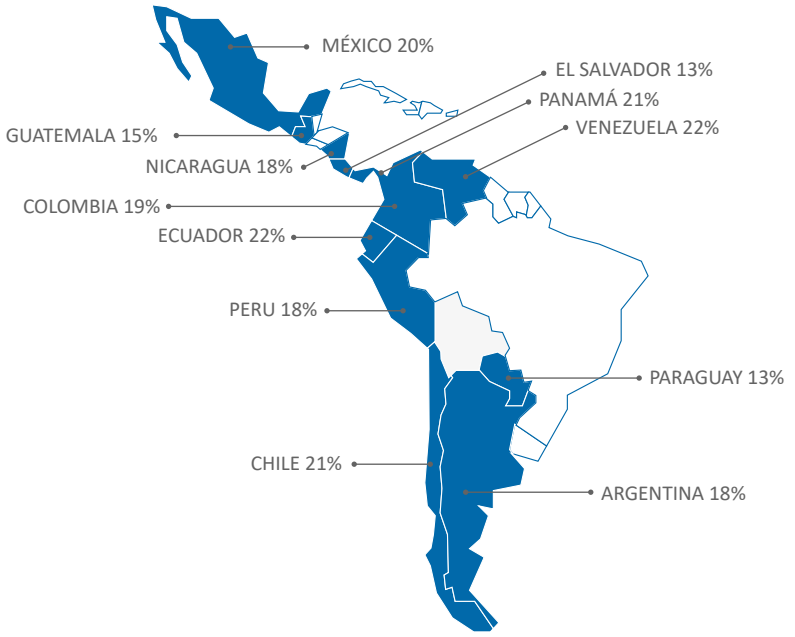
A la fecha la criminalidad digital sigue incrementándose, debo mencionar que esto obedece también a la falta de compromiso en la denuncia, hay suficientes razones para que el cibercrimen sea particularmente difícil de cuantificar y cuando obedece en las empresas la necesidad de proteger la reputación 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.

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.

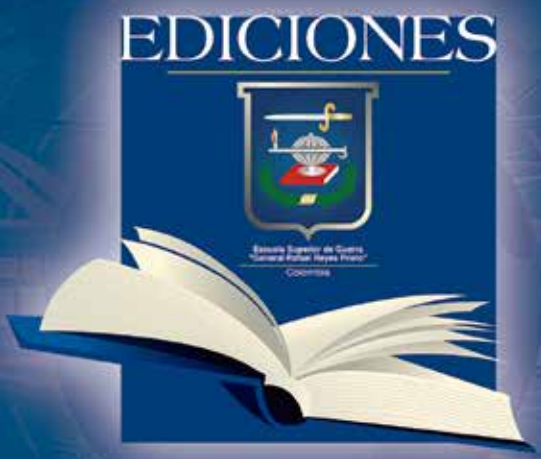
WSIS, Geneva 2003 - Tunis 2005, "Tunis Commitment," 18 November 2005, www.itu.int/net/wsis/docs2/tunis/off/7.html

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