Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia*

National Challenges for Cybersecurity on a Global Level: an Analysis for Colombia

Desafios nacionais da cibersegurança no cenário global: uma análise para a Colômbia

Fecha de recepción: 2019/03/30 | Fecha de evaluación: 2019/08/06 | Fecha de aprobación: 2020/08/27

Milton Ricardo Ospina Díaz
Magíster en Gestión de Organizaciones
Profesor, Facultad de Ciencias Económicas
Universidad Militar Nueva Granada
Profesor catedrático
Escuela Superior de Administración Pública
Bogotá, D.C., Colombia
milton.ospina@unimilitar.edu.co
ORCID: https://orcid.org/0000-0002-2194-3281

Pedro Emilio Sanabria Rangel
Doctor en Bioética
Profesor, Facultad de Ciencias Económicas
Universidad Militar Nueva Granada
Bogotá, D.C., Colombia
pedro.sanabria@unimilitar.edu.co
ORCID: https://orcid.org/0000-0001-7018-9417

Para citar este artículo / To reference this article / Para citar este artigo: Ospina, M., y Sanabria, P. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad*, 62(2), 199-217.

Resumen

En este artículo se aborda el tema de la seguridad de la información frente a amenazas cibernéticas en un contexto global, haciendo una revisión de la situación actual en Colombia. Mediante una investigación cualitativa, teórica, documental y descriptiva, se hace un recorrido histórico sobre la ciberseguridad (ciberguerra, ciberdefensa, delitos informáticos), particularmente en el componente de seguridad de la información, y se trabajan diversos aspectos al respecto (contextos, análisis de riesgos, sistemas de gestión y estándares de calidad) mientras se muestran los riesgos para las empresas, la sociedad y los países, evidenciados con la pandemia del coronavirus (COVID-19). Para el caso colombiano se revisaron datos sobre las acciones gubernamentales ante estas amenazas y se indagó sobre sus políticas de seguridad informática y estándares de calidad. Al final del artículo se muestran los retos que tiene Colombia frente a las amenazas cibernéticas, en cuanto a la seguridad de la información.

Palabras clave

Delito informático, criminología, criminalidad, criminalidad mediante computadoras (fuente: Tesauro de Política Criminal Latinoamericana - ILANUD). Guerra cibernética, piratería informática, hackers, organizaciones públicas (autor).

* Artículo derivado del trabajo de la línea de investigación en "Estrategia y control de gestión" del Grupo de Estudios Contemporáneos en Gestión y Organizaciones de la Universidad Militar Nueva Granada.

Abstract

This article covers the topic of information security in light of cybersecurity threats in a global context, reviewing the current situation in Colombia. A historical walk-through on cybersecurity was performed through qualitative, theoretical, documentary and descriptive research (cyberwar, cyberdefense, computer crime), particularly in the component of information security. In addition, various aspects in that regard were worked on (contexts, risk analyses, management systems and quality standards), while risks to businesses, society and countries are shown, demonstrated with the coronavirus (COVID-19) pandemic. In the case of Colombia, data on government action in light of these threats were reviewed and its information security policies and quality standards were researched. Colombia's challenges from cybersecurity threats, in terms of information security, are shown at the end of the article.

Keywords:

Computer crime, criminology, criminality, crime through computers (source: Latin American Criminal Policy Thesaurus - ILANUD). Cyber warfare, software piracy, hackers, public organizations (author).

Resumo

Este artigo aborda o tema da segurança da informação contra ameaças cibernéticas em um contexto global, fazendo uma revisão da situação atual na Colômbia. Através de uma pesquisa qualitativa, teórica, documental e descritiva, faz-se um percurso histórico sobre a cibersegurança (ciberguerra, ciberdefesa, crimes informáticos), particularmente no componente de segurança da informação, e trabalham-se vários aspectos a este respeito (contextos, análise de riscos, sistemas de gestão e padrões de qualidade), enquanto mostram-se os riscos para as empresas, a sociedade e os países, evidenciados pela pandemia de coronavirus (COVID-19). No caso colombiano, foram revisados dados sobre as ações do governo diante dessas ameaças e foi feita uma pesquisa sobre as políticas de segurança informática e padrões de qualidade. Os desafios que a Colômbia enfrenta diante das ameaças cibernéticas, em termos de segurança da informação, são mostrados ao final deste artigo.

Palavras-chave

Delito informático, criminologia, criminalidade, criminalidade através de computadores (fonte: Tesauro de Política Criminal Latino-Americana - ILANUD). Guerra cibernética, pirataria informática, hackers, organizações públicas (autor).

Introducción

Fruto del desarrollo que ha tenido la tecnología, ahora cotidiana, tanto de los individuos (utilización de dispositivos móviles, redes sociales, Internet 5G) como de las organizaciones privadas y públicas (gobierno digital, datos abiertos, Software de Gestión Empresarial ERP, Intercambio Electrónico de Documentos -EDI, Sistemas de Información Geográficos -SIG-, *big data*, inteligencia artificial -IA- e inteligencia de negocios -BI), han surgido transformaciones significativas para la humanidad (interpretadas como avances).

Este desarrollo tecnológico (internet, sistemas de información y nuevas tecnologías) ha generado en la sociedad rápidas transformaciones, crisis sociales, tensiones políticas, cambios culturales, problemas ambientales, transformaciones en mercados, etc., y revoluciones sin precedentes en diferentes ámbitos (educación, entretenimiento, trabajo y relaciones sociales, entre otros). No obstante, las tecnologías que se consideran señales del progreso también han generado problemas (dependencia tecnológica y vulnerabilidad de información). De esta manera, los medios tecnológicos, las telecomunicaciones, las aplicaciones móviles, las transacciones electrónicas, entre otras, han generado un sinnúmero de peligros asociados a la comisión de delitos informáticos (por personas u organizaciones inescrupulosas), en cuanto facilitan el ataque y aprovechamiento de las vulnerabilidades de individuos, empresas y/o gobiernos. Esta situación adquiere gran

relevancia si se considera el incremento en la frecuencia de los ataques a la información, la seguridad, la integridad y la dignidad de las víctimas.

En la actualidad los sistemas de información, la internet y la computación en la nube son el soporte para el almacenamiento, gestión y aplicación de información personal y organizacional, convirtiéndose en el blanco para quienes la quieren robar, manipular o dañar, o desean afectar a sus propietarios. Esto se presenta porque las personas y las organizaciones soportan su rutina en esta información, de manera que cualquier manipulación o fallo termina afectándolos notoriamente, a nivel individual y colectivo.

En este sentido, es posible imaginar las enormes implicaciones de que la información existente en correos electrónicos, redes sociales, reuniones privadas de trabajo o estudio o archivos laborales sufran ataques, daños o pérdidas; los efectos de fallas en bases de datos, edificios inteligentes o sistemas de inventarios, clientes, proveedores o nómina de una organización; las consecuencias de que se vulnere la integridad de una persona debida a la manipulación de información o la suplantación en redes (Amato *et al*., 2018); o los impactos del mal funcionamiento de sistemas de infraestructura crítica de servicios (represas, plantas de energía, aeropuertos, etc.) o de la pérdida de información estratégica del Estado o de entidades de la administración pública, a nivel central o subnacional. Todas estas cuestiones y preocupaciones componen el campo de la ciberseguridad.

Los antecedentes del tema se encuentran en la Guerra Fría y en la sensación de peligro que se tenía frente a la posible destrucción mutua entre Estados Unidos y la Unión Soviética, que podría haber afectado la vida de millones de seres humanos y la integridad de diversos países. Con ese riesgo latente, el Departamento de Defensa de Estados Unidos desarrolló un modelo (red) de transferencia virtual de datos a distancia (Arpanet), precursor de internet (Gaitán, 2014), que facilitó el tránsito de información entre los actores de la guerra. En la actualidad esta red es ampliamente utilizada con fines civiles y comerciales y se convirtió en la plataforma para toda actividad humana contemporánea. Sin embargo, esta "red de redes" también es un espacio con riesgo significativo que constituye la quinta dimensión de la guerra (la primera es la tierra; la segunda, el mar; la tercera, el aire; la cuarta, el espacio; la quinta, el ciberespacio), por lo cual el escenario asociado a ella se ha llamado ciberguerra, que sobrepasa lo previsto para las guerras de cuarta y quinta generación (Osorio, 2017).

Esta nueva dimensión bélica se ha constituido en un espacio de influencia y de dominación asimétrica entre individuos, empresas o Estados, puesto que cualquiera puede realizar espionaje, afectar actividades cotidianas o vitales o, incluso, causar daños a otros, mediante el uso de un ordenador, internet y conocimientos informáticos. Un ejemplo de ello se puede observar en los presuntos ciberataques a las elecciones presidenciales de 2016 en Estados Unidos y a los procesos electorales de diversos países, que se suman a la línea de acción iniciada a fines de la década del noventa, cuando ocurrieron muchos actos de sabotaje, espionaje y manipulación informativa en internet en varios países (El Diario, 2017). En la actualidad ya no parece necesario lanzar misiles o atacar físicamente una infraestructura (instalaciones, bases militares, estructuras de servicios, etc.), sino que puede generarse daño mediante la divulgación de información privada (infiltración) al menoscabar reputaciones y carreras políticas, neutralizar opositores, difundir secretos industriales o militares o sabotear páginas web y sistemas de información, entre otros, gracias a la manipulación, secuestro o destrucción de información personal o institucional.

Los gobiernos y los organismos de seguridad reconocen que en la actualidad existe más riesgo de vulneración a la seguridad, incluyendo los delitos informáticos, ciberterrorismo y las diversas amenazas cibernéticas (Reyna y Olivera, 2017) que han causado daños a la sociedad y pérdidas económicas. También por esto, la administración pública y las diversas organizaciones a nivel mundial han elevado sus capacidades tecnológicas de ciberdefensa y de seguridad de la información (mediante sistemas y protocolos de seguridad cada vez más sofisticados) para contrarrestar estos posibles ciberataques. Simultáneamente, se ha generado la necesidad de crear nuevas leyes, actualizar la legislación y establecer normas técnicas de calidad. El temor a estas situaciones (cibercatástrofes) ha incitado a que los países dediquen esfuerzos y recursos crecientes para gestionar la seguridad en el ciberespacio. Ejemplo de ello son los avances de China y Rusia por desarrollar su internet soberano.

En tal sentido, este artículo se propone analizar el tema de la seguridad de la información frente a las ciberamenazas y revisar la situación al respecto de los ciudadanos y las organizaciones públicas en Colombia. En la revisión de literatura sobre este tema, no se encuentran muchos estudios que muestren la perspectiva global sobre la ciberseguridad, y aun menos en el contexto colombiano. Al respecto, se encuentran los estudios de Marín, Nieto, Huertas y Montenegro (2019), quienes proponen un modelo de delitos cibernéticos (desde lo ontológico) en el cual se analizan las más recientes modalidades delictivas cibernéticas usadas en Colombia y se pretende aportar a la prevención y decisión frente a la seguridad cibernética. Por otra parte, Izycki (2018)

compara las estrategias nacionales de ciberseguridad de diez países latinoamericanos, incluyendo Colombia; y Eslava, Rojas y Pineda (2013) muestran que los sistemas de comunicación del sector eléctrico en el país no se encuentran preparados para contrarrestar ataques ciberterroristas, y plantean una propuesta para evitar esta problemática.

En relación con lo anterior, este artículo pretende cubrir parte de esta deficiencia y aportar al conocimiento sobre el tema, particularmente para el contexto colombiano. Se considera que puede aportar a la discusión académica, como soporte curricular de programas académicos relacionados y como referente para el diseño y revisión de las políticas públicas sobre ciberseguridad.

Se expone inicialmente la metodología. A continuación se desarrolla la ciberseguridad desde diferentes dimensiones (contexto, análisis de riesgos, sistemas de gestión de soporte y estándares de calidad asociados), incluyendo su aplicación en el contexto colombiano. Posteriormente, se muestran los resultados de la reflexión y, por último, se discuten los desafíos existentes para el país en cuanto a ciberseguridad.

El referente principal de la reflexión final es el concepto de reto (estratégico), que se refiere a los desafíos que se deben asumir frente a una situación y se enfoca hacia una política gubernamental que propugne por protegerse frente a vulneraciones en la infraestructura crítica de la nación, garantice los derechos de los ciudadanos en un mundo *online*, renueve la administración de justicia en el entorno digital, y contrarreste la inseguridad de la información en el contexto tecnológico y operacional (Cano, 2011).

Consideraciones metodológicas

Esta investigación asume la perspectiva interpretativa, pues le da significado a los hechos desde el punto de vista del investigador (Mertens, 2010), reconociendo la imposibilidad de eliminar su subjetividad. Se inscribe en el enfoque cualitativo porque pretende profundizar en el análisis, más que generalizar (Sutton, 2016).

Puede considerarse histórica, pues desarrolla una cronología de los hechos -seguridad de la información- (Tamayo, 2011), aunque con corte en un momento del tiempo y sin tomar datos de estudios previos (porque no se encuentran), haciendo improcedente la comparación -transversal-.

También puede denotarse como descriptiva al apoyarse, relacionar y contrastar estadísticas que muestren las características o manifestación del fenómeno (Tamayo, 2011) y como teórica, al efectuar un análisis crítico y sistemático de un problema teórico, de planteamientos de diversos autores, o de teorías ya desarrolladas (Hernández, 2002).

Es documental, pues en ella se recoge, clasifica, recupera y distribuye información (Ekman, 1989) a través de tres etapas: consulta documental, contraste de información y análisis histórico del problema (Amador, 1998).

El método usado es la revisión documental, empleando técnicas como el análisis documental, el análisis y la comparación, que partieron de una búsqueda en bases de datos documentales, particularmente Scopus -SciVal- (una de las más representativas). La combinación de búsqueda estuvo compuesta por las palabras "*cybersecurity*" y "Colombia", aplicadas en los campos de título, palabras claves y resumen. Esta combinación se concretó en la ecuación TITLE-ABS-KEY ("*cybersecurity*"+"Colombia"). La estructura presentada aquí se basa en la propuesta de Sanabria Rangel (2016).

Esta exploración, sin delimitación temporal, de campos de estudio, ni de tipo de documentos, arrojó solo seis documentos (publicados entre 2013 y 2019). Dada la clasificación realizada por Scopus, al analizar estos textos por campos de conocimiento se encuentra que tres de ellos corresponden al área de ciencias de la computación; dos a ingeniería; uno a negocios, gestión y contabilidad; uno a economía, econometría y finanzas; uno a matemáticas; y cinco en el área de ciencias de la computación (que incluye uno nuevo y otros pertenecientes también a otras áreas), lo que evidencia que no es una suma aritmética. Con otra óptica, se encuentra que dos corresponden a artículos, dos a revisiones de conferencia, uno a libro y uno a memorias de conferencia. Se seleccionaron aquellos que se consideraron significativos.

Después, mediante búsqueda en otras bases de datos, en fuentes de información diversa y medios institucionales y periodísticos, se seleccionaron aquellos textos considerados pertinentes para desarrollar la temática y que aportaran a la argumentación. Por tanto, aunque se hace uso de herramientas de revisión sistemática de literatura, el trabajo corresponde más con una revisión narrativa.

Sobre estos se realizó un análisis de contenido, apoyados en técnicas como fichas de lectura, cuadros comparativos y tablas analíticas, para extraer sus principales planteamientos, realizar la interpretación y generar los argumentos.

Ciberseguridad

La ciberseguridad (o seguridad informática) se origina para tomar medidas para la protección de infraestructura, software y hardware, contrarrestando las posibles amenazas mediante internet, y para desarrollar estrategias de contraataque. Esta perspectiva implicó la creación de sinnúmero de normas y sanciones para

mitigar los delitos a través de esta red (Reyna y Olivera, 2017). Por otro lado, la ciberseguridad alude al:

> Conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. […] La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios [disponibilidad, integridad, autenticidad, confidencialidad, etc.] contra los riesgos de seguridad correspondientes en el ciberentorno (ITU, 2010).

Su aplicación implica aspectos estructurales (elementos computacionales que generan capacidades, fuerza y dominio en el ciberespacio) y aspectos geopolíticos (elementos referidos al ejercicio del poder, las dinámicas sociales y los dominios sobre el espacio digital y en términos de superioridad) (Saavedra y Parraguez, 2018a), pues estos son los que han venido a hacer presencia en las confrontaciones.

Algunos afirman que la ciberseguridad es un concepto de ingeniería social, por lo cual se ha propuesto realizar estudios concretos sobre el concepto que permitan avanzar en su comprensión (Hatfield, 2018). Algunos aspectos relacionados con el tema son el contexto global, la ciberseguridad y los riesgos vinculados, los sistemas de gestión asociados y la norma ISO 27001.

La ciberseguridad en el escenario global

Los problemas de ciberseguridad (derivados de la ciberguerra) se caracterizan porque en ellos no se pueden detectar claramente los bandos en contienda, puesto que pueden involucrar acciones de gobiernos contra sus ciudadanos, de partidos políticos contra sus opositores, de corporaciones contra sus competidores, de ejércitos contra sus enemigos, etc.

Por otra parte, la ciberseguridad ha terminado siendo un asunto global pues el ciberespacio no tiene arraigo en ningún país y por ello el ecosistema digital, y su protección frente a las actividades ilícitas, terminó siendo un asunto que atañe a todas las naciones y sin fronteras claras. Por ello se plantean discusiones sobre la regulación del ciberespacio, la gobernanza en él y la defensa unilateral (Saavedra y Parraguez, 2018b).

Al revisar los antecedentes se encuentran una serie de incidentes cibernéticos importantes a nivel mundial (Tabla 1).

Tabla 1.
Incidentes cibernéticos internacionales (2003-2020)

Año	Incidente
2003	Acusación de EEUU a China sobre ataques informáticos (Titan Rain).
2007	Ataques a Estonia que inutilizaron infraestructuras críticas.
2008	Explosión, por ataque cibernético, del oleoducto BTC en Refahiye (Turquía).
2010	El gusano informático *Stuxnet* genera daños en plantas de uranio iraníes y sabotea proyectos estratégicos nacionales.
2012	Borrado de 30.000 discos duros de la empresa petrolera Saudí Aramco.
2016	Presunto ciberataque ruso (servicios de seguridad rusos) en las elecciones presidenciales de EEUU con filtraciones de información de los servidores de correo del Comité Nacional Demócrata y de su candidata Hillary Clinton, publicación de documentos para afectar su imagen y posible manipulación de elecciones en favor de Donald Trump.
2018	Supuestos ciberataques contra estructuras de información de Rusia en la copa mundial de futbol y contra redes de suministro eléctrico en 2019.
2019	Presuntos ataques cibernéticos a la infraestructura eléctrica de Venezuela.
2020	Acusaciones entre potencias por presuntos ataques cibernéticos para robo de propiedad intelectual e información sobre vacunas COVID 19.
2020	Intrusión a la plataforma de videoconferencias Zoom para extraer información, infiltrar datos y boicotear reuniones remotas.

Fuente: elaboración propia.

Este nuevo escenario de riesgos, frente al tema de la ciberseguridad, incluye a países como Estados Unidos, China, Rusia, Irán, India, Alemania, Irlanda, Corea del Norte y Corea del Sur, entre otros. Un ejemplo de la forma como se ha desarrollado el tema a nivel mundial se ve en el planteamiento de Clarke y Knake (2011) en el que se muestra cómo China, debido al seguimiento que hicieron al desarrollo de la operación "Tormenta del Desierto" en el Golfo Pérsico (con manifestación del enorme poderío militar norteamericano), generó una estrategia nacional para desarrollar mecanismos para enfrentarse en igualdad de condiciones con Estados

Unidos, en caso de un conflicto. Por ello, China ha dedicado cuantiosos recursos a la investigación de nuevas tecnologías, entre ellas el desarrollo de las armas cibernéticas (Stevens, 2018).

Más allá de esto, los problemas de ciberseguridad se manifiestan también en ataques directos a las corporaciones, bien mediante espionaje o difundiendo su información confidencial, ya sea por razones políticas, financieras o sociales. Algunos ejemplos son el jaqueo a la empresa italiana Hacking Team Labs, la divulgación de correos electrónicos de la empresa Sony, la publicación por parte de Edward Snowden de información confidencial de la National Security Agency (NSA) (en el caso denominado "*climategate*"), o el saboteo de las marcas de tarjetas de crédito a WikiLeaks.

Esta última fue mencionada también por los medios de comunicación, intensamente, por los escándalos que generó por la divulgación de información clasificada de personas y organizaciones. WikiLeaks[1] terminó analizando y publicando datos censurados o material clasificado que incluye información sobre guerras, espionaje y corrupción (WikiLeaks, 2015).

Adicionalmente se encuentra el escándalo de los Panamá Papers (2016), que muestran el funcionamiento de los paraísos fiscales y el movimiento secreto del dinero en el mundo. En total, 140 políticos de 50 países aparecieron vinculados con este manejo, entre ellos 12 presidentes y numerosas personalidades (Telesur, 2016).

Otra manifestación es el incidente informático (2017) en el que varias compañías y entes gubernamentales mundiales fueron blancos de un ataque cibernético a gran escala que bloqueó las actividades de las computadoras para pedir recompensas mediante *bitcoin* (criptomonedas). Según la firma de antivirus rusa Kaspersky, este virus informático infectó sistemas operativos en Francia, Rusia, Reino Unido, Estados Unidos, Dinamarca, Alemania, India, España, Brasil, Colombia y Ucrania.

Este virus terminó afectando también la agencia británica de publicidad WPP, el Banco Central ucraniano, la más grande productora petrolera rusa Rosneft, la compañía naviera danesa Maersk, el fabricante de aeronaves de Ucrania Antónov, la productora de alimentos española Mondelez, la naviera holandesa TNT, la compañía francesa de materiales para construcción Saint-Gobain, la farmacéutica estadounidense Merck y la firma de abogados colombiana DLA Piper (BBC Noticias, 2017).

Hechos más recientes son el jaqueo de la plataforma de videoconferencias Zoom, que en el marco de la pandemia por el COVID-19 tomó gran relevancia y tuvo un crecimiento sin precedentes por el amplio uso que le ha dado en empresas, colegios, universidades y otras organizaciones para reuniones remotas, que fue vulnerada mediante Zoom *bombing*. Estos actos comprometieron y expusieron gran cantidad de cuentas, usuarios y claves (alrededor de 500.000) y afectaron las actividades personales, académicas y laborales de muchas personas y organizaciones, al permitir el acceso no autorizado a reuniones privadas para extraer datos, infiltrar información, para divulgar información falsa, grosera, discriminatoria o pornográfica, o para sabotear. Todo ello derivado, aparentemente, de la venta de cuentas, usuarios y contraseñas de la plataforma en la red oscura (El Universal, 2020).

Otros hechos recientes son la filtración de contraseñas de la Organización Mundial de la Salud (OMS), la Fundación Gates y el Instituto Nacional de Salud de Estados Unidos, que divulgó información atribuyendo la creación del Coronavirus al laboratorio chino P4 (El Universal, 2020) o las acusaciones hechas por Reino Unido y EEUU a jáquers de Rusia y China, respectivamente, en el marco de la carrera existente entre potencias por desarrollar la vacuna contra el coronavirus, que denuncian presuntos ciberataques para obtener la información sobre avances al respecto y los tratamientos para el COVID-19. Aunque los gobiernos acusados niegan su participación, este episodio derivó en el cierre del consulado chino en Houston (Revista Semana, 2020).

Todo esto muestra la generalización del fenómeno y es ratificado por el estudio anual Cyber Resilient Organization (2018) que muestra que un 77% de las organizaciones no están preparadas para enfrentar los ataques cibernéticos y que tampoco tienen un plan consistente de respuesta ante dichas amenazas (IBM, 2018).

En consecuencia, los países y las organizaciones supranacionales han dirigido sus esfuerzos a contrarrestar acciones similares y han originado agencias gubernamentales encargadas de la seguridad informática. En Estados Unidos se creó el Computer Emergency Response Team Coordination Center (como un centro de alerta y reacción frente a estos ataques); en España está el Instituto Nacional de Ciberseguridad (INCIBE); en la Unión Europea se encuentra el Centro Europeo de Ciberdelincuencia; en Alemania se cuenta con el Centro Nacional de Defensa Cibernética; en México se tiene la UNAM CERT (como un grupo de profesionales que evalúa vulnerabilidades en los sistemas de Información en México); en la OTAN se creó el Cyber Defence Management Authority (CDMA). En Colombia está el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), con participación del Ministerio

1 WikiLeaks es una organización multinacional de medios de comunicación, sin fines de lucro, fundada en 2006 por el editor y periodista australiano Julian Assange.

de Tecnologías de la Información y las Comunicaciones (MinTIC) y la Policía Nacional de la República de Colombia (Colcert, 2017).

El esfuerzo mundial se encuentra en la Agenda de la International Telecommunication Union (ITU) (Global Cybersecurity Agenda -GCA-), con 193 Estados miembros, que pretende afrontar el fenómeno de ciberseguridad en sus cinco pilares (legal, técnico, organizativo, creación de capacidades y cooperación).

Esta agencia genera periódicamente el índice global de ciberseguridad que muestra el estado del tema en países y regiones. Los resultados más recientes muestran el compromiso y trabajo de todos los países respecto a ciberseguridad, el fortalecimiento del tema en naciones de todas las regiones (aunque con algunas brechas entre ellos) y la necesidad de trabajar en acciones de mejora sobre cooperación, creación de capacidades y organización. Resalta el caso de África y América, que presentan los mayores desafíos, requiriendo de mayor participación y de apoyo continuo (ITU, 2017), a pesar de las estrategias implementadas en la región para fortalecer el tema (Hernández, 2018). Todo ello se da enmarcado en las discusiones sobre la necesidad de intervención de los Estados sobre el manejo de la información, los niveles y restricciones de acceso y uso de esta, pero que podría limitar las libertades individuales (Koch, 2015).

En cuanto a personas, se presentan también afectaciones graves por estos delitos cibernéticos. Un ejemplo es el juego ruso nombrado "reto de la ballena azul" (2017) que mundialmente invitaba a los niños y adolescentes a hacerse daño físico y psicológico, llevándolos incluso al suicidio, o la FaceApp de envejecimiento (2019) que robaba datos personales (Vanguardia, 2019). En Colombia se estimó que en 2020 los ataques cibernéticos podrían afectar a 4.000 millones de personas (Policía, 2017d).

Esto se ha hecho tan relevante que se calcula que la inversión mundial en seguridad cibernética se duplicará entre los años 2016 y 2021 (rebasando los 6 trillones de dólares) y que los empleos relacionados se triplicarán (pasando de 1 a 3,5 millones en este mismo periodo). Esto se relaciona con el aumento global en el número de internautas (pasó de 2.000 a 3.800 millones entre 2015 y 2017) y que se estima llegará a 6.000 millones en 2022 (Oppenheimer, 2018).

Como se observa, la ciberseguridad va a transformar las formas de trabajo, a generar nuevos perfiles de cargos y a crear nuevos programas académicos relacionados pues se prevé que en 2022 se requerirán 3,5 millones de profesionales en ciberseguridad (Jordan y Dixon, 2018). También los salarios de los expertos empiezan a superar el de muchas profesiones.

Ciberseguridad y análisis de riesgos informáticos

La ciberseguridad se enfoca entonces en la protección de la infraestructura computacional y de la información circulante en las redes informáticas, aunque también del diseño de normas, procedimientos, métodos y técnicas que posibiliten seguridad y confiabilidad en los sistemas de información. Esto es importante pues los ataques en el ciberespacio afectan no solo en el mundo digital sino que pueden concretarse en el ámbito físico, por ejemplo, dañando sistemas estructurales de una organización, una nación o una región (Saavedra y Parraguez, 2018b).

Por ello, actualmente se cuenta con estándares, protocolos, métodos, reglas, herramientas y normas para minimizar los riesgos y amenazas cibernéticas, que comprenden *software*, programas, bases de datos, archivos y *hardware*. Entre las normas de seguridad informática se encuentran también horarios de funcionamiento, restricciones de acceso, autorizaciones y denegaciones, perfiles de usuario y planes de emergencia.

No obstante, las amenazas a la seguridad informática aparecen principalmente debido a: a) usuarios con permisos sobredimensionados, sin restricción a accesos innecesarios; b) programas maliciosos; c) errores de programación; d) acceso de intrusos; e) generación de siniestros, robos e incendios; f) acceso de personal técnico interno; g) catástrofes naturales, o h) ingeniería social (errores humanos, falta de precaución al compartir contraseñas, claves, códigos o por descarga de archivos) (Incibe, s.f.). Un riesgo adicional se encuentra en la estrategia de efectuar ataques con baja tasa ("bajo perfil") y que terminan siendo más efectivos pues generan menor posibilidad de detección (Sawyer y Hancock, 2018).

Debido a ello, algunas legislaciones se centran en implantar políticas de seguridad de la información que impidan su pérdida o robo en organizaciones públicas y privadas (Incibe, s.f.) y que cumplen múltiples criterios técnicos. Como complemento, en torno al tema de ciberseguridad se ha incorporado el proceso de análisis de riesgos informáticos, que comprende la identificación de activos informáticos, sus amenazas y vulnerabilidades, su probabilidad de ocurrencia y su impacto, buscando determinar los controles adecuados para evitar, minimizar y transferir el riesgo de daños o pérdidas para personas y organizaciones. Entre los muchos modelos existentes se encuentra el de Henriques, Silva, Poleto, Camara, y Cabral (2018).

Estos controles deben implantarse mediante un esquema de protección que preserve al sistema y la confidencialidad, integridad y disponibilidad de los datos. Para ello se hace uso de la *matriz de riesgo* en la cual

se ubican los factores identificados y sus relaciones para determinar objetivamente los riesgos relevantes en seguridad de la información, al igual que el nivel de riesgo ante posibles ataques informáticos, permitiendo contrastar la probabilidad de ocurrencia con los posibles impactos. Esto facilita proponer acciones concretas que minimicen los riesgos y estimar su impacto sobre la seguridad de la información. La fórmula para estimar este riesgo total es:

RT (*Riesgo Total*) = *Probabilidad x Impacto Promedio*

En la Figura 1 se ejemplifica una gráfica derivada de esta matriz en la que se observa la existencia de riesgo de nivel medio alto (punto ubicado en el plano).

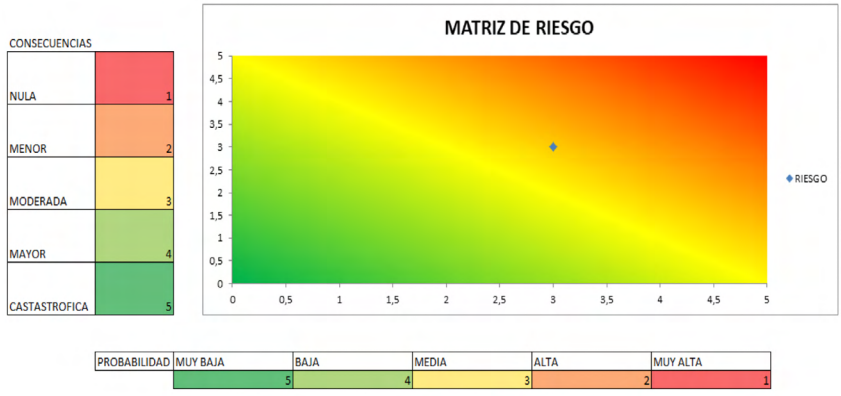

Figura 1. Ejemplo de gráfica de evaluación de una matriz de riesgo.

Fuente: Elaboración propia.

Como complemento, internacionalmente se generó el marco para la mejora de la seguridad cibernética en infraestructuras críticas (Barrett, 2018), cuya estructura en cinco funciones se plantea con un lenguaje común y metodologías que permiten abordar y administrar el riesgo de seguridad cibernética, al identificar y priorizar acciones de mitigación (Tabla 2):

Tabla 2.
Marco para ciberseguridad

Función	Categoría
Identificar	• Gestión de activos • Entorno empresarial • Gobernanza • Evaluación de riesgos • Estrategia de gestión de riesgos • Gestión de riesgo de la cadena de suministro
Proteger	• Gestión de identidad y control de acceso • Conciencia y capacitación • Seguridad de datos • Procesos y procedimientos de protección de la información • Mantenimiento • Tecnología protectora
Detectar	• Anomalías y eventos • Vigilancia continua de seguridad • Procesos de detección
Recuperar	• Planificación de recuperación • Mejoras • Comunicaciones

Fuente: Barrett (2018).

Sistemas de gestión de ciberseguridad para la información

Como se hace evidente, es imposible un nivel de protección total frente a los delitos cibernéticos, incluso cuando existe un enorme presupuesto. No obstante, la implementación de los Sistemas de Gestión de Seguridad de la Información (SGSI) es fundamental para ello, pues contribuye a que los riesgos cibernéticos sean conocidos, asumidos, gestionados y minimizados de forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a las modificaciones en los riesgos, entorno y nuevas TIC.

Un SGSI contempla los procedimientos y planifica e implanta controles de seguridad basados en una evaluación de riesgos y en una medición de su eficacia (ISO, 2005). Por ello se indica que este sistema de gestión debe contemplar elementos como el manual de seguridad, los procedimientos, las instrucciones, los *checklist*, los formularios y los registros sobre la información y que deben fundamentarse en el desarrollo del ciclo PHVA como base para su implementación y gestión (que resulta reiterativo en los diversos sistemas de gestión de la calidad).

Por supuesto, el SGSI puede integrarse con otras normas de calidad como ISO 9001, ISO 14001 e ISO 45001 (antes OHSAS 18001), aunque existen otros estándares internacionales al respecto: la guía para el desarrollo de una estrategia de ciberseguridad nacional (ITU, 2018), la revisión de los avances frente a las políticas para la protección de infraestructura e información crítica (OECD, 2019) y el Reglamento General de Protección de Datos (GDPR), con el que la Unión Europea (UE) tiene la intención de reforzar y unificar la protección de datos para todos los individuos allí (European Parliament y Council of the European Union, 2016), entre otros. Este último también se ocupa de la exportación de datos personales fuera de la UE. En ese marco, cada país cuenta con una Asociación de Protección de Datos (DPA), que es responsable del cumplimiento de la General Data Protection Regulation (GDPR) (Powerdata, 2019).

La ISO 27001

La norma internacional específica para los sistemas de gestión de la ciberseguridad y de la seguridad de la información es la ISO/IEC 27001 (ISO, 2005), emitida por la International Standards Organization (ISO) y la International Electrotechnical Commission (IEC), la cual tiene su primera versión en 2005 y se fundamenta en la norma BS 7799-2. Su versión más reciente es de 2013, aunque su documento conceptual se actualizó en 2018 (ISO, 2018).

Este es el principal estándar mundial sobre seguridad de la información, con un amplio abanico de aplicación (organizaciones con o sin fines de lucro, privadas o públicas, pequeñas o grandes), que proporciona una metodología para implementar la gestión de la seguridad de la información para reducir los riesgos hasta un nivel aceptable y dándole la posibilidad de certificarse, como ha ocurrido mundialmente con muchas empresas (ISO, 2005).

En la encuesta anual realizada por la ISO (2005) a nivel global (consulta a los organismos de certificación sobre número de certificados generados) se observa que finalizando 2016 ya existían 33.290 certificados otorgados (21% más frente al 2015, cuando había 27.536). Para el 2015, un 44% de registros estaban en el este de Asia y Pacífico, 38% en Europa, 9% en Asia Central y Sur, 5% en Norteamérica, 2% en Medio oriente, 1% en América Central y del Sur y 0.5% en África. Japón encabeza con 8.240 registros; en Latinoamérica, México lidera con 104, seguido de Colombia con 103, Brasil con 94, Argentina con 52, Chile con 32, Perú con 22 y Uruguay con 21 (Datasec, s.f.). Esto evidencia una brecha entre países en vías de desarrollo y los denominados países del primer mundo.

Este marco brinda tranquilidad a los diversos grupos de interés sobre la protección de la integridad de sus datos y sistemas, muestra compromiso con la seguridad de su información, genera oportunidades de negocio, mejora los estándares éticos de los empleados y reduce los riesgos de fraude, pérdida de datos o divulgación de información no deseada, entre otros beneficios.

Colombia y ciberseguridad

Colombia tampoco ha sido ajena a los ciberataques y, a pesar de los evidentes riesgos, se sabe que cerca del 43% de las empresas colombianas no están preparadas para enfrentarlos, lo cual ha impactado negativamente en muchos frentes, incluido el económico, pues solo en 2015 Colombia registró pérdidas por cerca de 1 billón de dólares por ciberataques (Revista Dinero, 2016). En consecuencia, en 2017 el país vio afectadas más de 12 empresas por el ciberataque mundial de un *ramsomware* que secuestraba información para exigir pagos en *bitcoins*, siendo más potente que su predecesor Wanna Cry (El Tiempo, 2017) y que llegó a afectar incluso entidades públicas como el Instituto Nacional de Salud (El Heraldo, 2017). Adicionalmente, estos delitos presentan bajo índice de denuncia pues solo un 40% son reportados, aunque solo en 2016 se recibieron 7.118 denuncias al respecto.

La situación en organizaciones privadas se observa en el estudio denominado *Impactos de los incidentes de*

seguridad digital en Colombia 2017, trabajado entre OEA y MinTIC[2] . Allí se destaca que el 70% de las grandes empresas sí se sienten *muy preparadas o preparadas* para un incidente digital, frente a un 45% de las microempresas y un 22% de todas las empresas consideran estar en *nivel medio de preparación*. El 37% de microempresas, 58% de pequeñas, 64% de medianas y 58% de grandes empresas solo tienen un departamento de TI para encargarse de la seguridad digital y solo el 22% de micro, 18% de pequeñas, 7% de medianas y 21% de grandes empresas indicaron que tenían un área específica de seguridad digital. En cuanto a la evaluación del riesgo cibernético, la industria lo evalúa con 50%, el comercio con 32% y los servicios con 45% (MinTIC, 2017d).

Adicionalmente, están los ciberdelitos asociados con el uso de internet para la intimidación, ridiculización, amenazas, extorsión y sextorsión (priorizando niños y adolescentes) y cuyos réditos se monetizan frecuentemente en criptomonedas, por tener menor regulación. Según el balance de cibercrimen en Colombia (Policía Nacional de Colombia, 2017a), estos delitos se presentan mayoritariamente en las ciudades principales y han venido incrementando. En 2017 los principales delitos informáticos fueron la ciberinducción al daño físico (508 alertas); la estafa por suplantación de *simcard* (pérdidas cercanas a los $7.690'000.000); el *vishing* (tráfico de datos financieros personales) (afectación por $2.132'000.000); el fraude por falso WhatsApp (381 casos); las ciberpirámides (montos cercanos a 1.500 millones de pesos); el *ransomware* (usado para atacar entidades públicas como el Instituto Nacional de Salud); el *carding* (comercialización de datos de tarjetas crédito y débito) (pérdidas cercanas a $60.000'000.000); las ventas ilícitas en internet; y la pornografía infantil, entre otros (Policía Nacional de Colombia, 2017c).

En los últimos años el centro cibernético policial ha recibido reporte de 15.565 delitos informáticos a personas y organizaciones que muestran un incremento (Policía Nacional de Colombia, 2017b). En 2014 los delitos contra ciudadanos llegaban al 92%, en 2015 al 63% y en 2016 al 57%, mientras que contra empresas pasó de 5% a 28% en ese periodo. El desarrollo del internet en el país ha favorecido este fenómeno, con una penetración del 34,52% en la población, alcanzando 16'898.138 de suscriptores a internet en 2017 (62,59% en internet móvil) (MinTIC, 2017a). Otro factor detonante es el crecimiento en el uso de correo electrónico, redes sociales, comercio electrónico y aplicaciones bancarias, entre otros.

Ya en 2019 se llegó a 30.410 delitos informáticos denunciados (54% más que en 2018) y se distribuyen en: *phishing* (42%), suplantación de identidad (28%), *envió* de *malware* (14%) y fraudes en medios de pago *online* (16%) (principalmente en Bogotá, Cali, Medellín y Barranquilla). Este año tomó auge la duplicación de perfiles de Facebook con fines de estafa, recibiéndose más de 1.000 denuncias (RED+, 2019), el uso del *ransonware* aumentó 500% en el país (Colombia ocupa el quinto puesto en la región en su índice de propagación), la modalidad del Business Email Compromise (BEC), o estafa sofisticada, dejó pérdidas estimadas en US$130.000, el *skimming* (fraude en cajeros electrónicos) registró 84 incidentes y la comercialización de estupefacientes en redes sociales llegó a 280 casos detectados. Ese mismo año, las grandes y medianas empresas reportaron cerca de 14'000.000 de intentos de ciberataques (correos fraudulentos, suplantación de identidad, enmascaramiento de correos e infección de sitios web) (El Tiempo, 2019).

En el informe *Tendencias de cibercrimen en Colombia (2019-2020)* se indica que los criminales están usando inteligencia artificial, por ejemplo, para enviar audios o videos a empresas suplantando a ejecutivos, clientes y proveedores para realizar transferencias monetarias (Policía Nacional de Colombia, 2019). De esta forma, se puede observar que el cibercrimen ya no es realizado espontáneamente por individuos aislados, sino que es cometido de manera estructurada por organizaciones delincuenciales muy especializadas, con carácter transnacional, que hacen segmentación y ubicación de las posibles víctimas a través de las redes sociales y que despliegan gran variedad de técnicas de seguimiento.

La vulnerabilidad frente a la ciberdelincuencia aumentó en 2020 debido al confinamiento preventivo derivado de la aparición del coronavirus (COVID-19), como consecuencia del aumento en la virtualización de la vida y el trabajo: clases remotas en colegios y universidades, incremento en el uso de aplicaciones de mensajería, aumento de transacciones bancarias *online*, compras por internet, comunicación de información por correo, expedición de documentos *online*, reuniones de trabajo con apoyo en TIC y diversas aplicaciones, entre otros. Aprovechando el aumento en el uso de medios virtuales y la imposibilidad de desplazamiento, se ha incrementado el uso de páginas falsas, textos desinformativos, mensajes con virus adjuntos y llamadas engañosas para apropiarse de datos bancarios (El Tiempo, 2020). Para ello se valen del uso de dominios falsos relacionados con el COVID-19, correos electrónicos con *phishing* informando sobre la pandemia, mensajes sobre ayudas financieras, comunicados divulgando devolución de impuestos, mensajes SMS con enlaces a aplicaciones malignas, etc. De igual manera, las organizaciones también

2 En él participaron 515 organizaciones empresariales (21% grandes, 12% medianas, 23% pequeñas y 44% microempresas, 69% servicios, 20% comercio y 11% industria).

están siendo hackeadas, aprovechando las debilidades de los sistemas domésticos de los trabajadores que laboran desde casa (sin cortafuegos, políticas de seguridad, ni filtros que limiten el descargue de aplicaciones, lo que implica un alto riesgo) (Noticiero CM&, 2020).

Por su parte, las plataformas gubernamentales tampoco escapan a estos ataques ni han podido evitar el uso de su nombre para cometer delitos, por ejemplo, en el envío de falsos correos. Esto ha afectado a organizaciones estatales como la DIAN, la Fiscalía General de la Nación, el SIMIT (tránsito), etc. Así, los delincuentes han logrado que los ciudadanos descarguen archivos (*malware*) que les permiten acceder a los equipos para sustraer, secuestrar o destruir información. Por esta tendencia, en 2018 y 2019, altos funcionarios del gobierno de Colombia y de la Organización del Tratado del Atlántico Norte (OTAN) se reunieron para abordar el tema de la ciberdefensa y la ciberseguridad.

Ante estos desafíos de seguridad digital, las organizaciones estatales no se encuentran en buena situación, en la mayoría de los sectores en que se encuentran (política estatal No. 7), pues su calificación promedio al respecto fue de 74,2 y 77,8 para los años 2018 y 2019, respectivamente, aunque algunos sectores sí registran calificación superior a 80 (Reporte de Resultados Sectoriales de Desempeño Institucional Nación sobre seguridad digital en el Formulario Único Reporte de Avances de la Gestión -FURAG-, en el marco de Modelo Integrado de Planeación y Gestión -MIPG-) (Tabla 3).

Tabla 3.
Resultados desempeño en seguridad digital (2018-2019) en entidades estatales por sector

Sectores Gobierno Colombia	Puntaje promedio por sector 2018	Entidades consultadas	Puntaje promedio por sector 2019	Entidades consultadas
Relaciones Exteriores	87	2	89,4	2
Comercio, Industria y Turismo	82	9	82,7	9
Tecnologías de la Información y las Comunicaciones	81	6	76,1	7
Presidencia de la Republica	81	5	79,9	5
Ciencia, Tecnología e Innovación	79	1	82,6	1
Planeación	79	4	83,9	4
Hacienda y Crédito Público	79	18	84	18
Educación	78	10	86,4	10
Inclusión Social y Reconciliación	75	4	83	4
Función Pública	74	2	70,6	2
Defensa	74	16	79,7	17
Justicia y Derecho	74	5	77,1	5
Ambiente y Desarrollo Sostenible	74	4	79,2	4
Minas y Energía	74	6	77,1	6
Vivienda, Ciudad y Territorio	73	3	81,1	3
Salud y Protección Social	73	9	77,5	10
Trabajo	72	6	78,2	6
Estadísticas	70	2	67,7	2
Agropecuario, Pesquero y de Desarrollo Rural	69	13	72,6	13
Cultural	67	4	71,5	4
Del Deporte, la Recreación y el Aprovechamiento del Tiempo	65	1	57,4	1
Transporte	65	7	79,4	6
Interior	61	6	71,5	6
Total	**74,2**	**143**	**77,8**	**145**

Fuente: Departamento Administrativo de la Función Pública (2019).

Como se observa existe una mejora para 2019 frente a la seguridad digital de los diferentes sectores estatales. Esto se debe gracias a la creciente normatividad y a la preocupación gubernamental por contrarrestar estas ciberamenazas, que se hace manifiesta en estrategias como el programa *Agenda Estratégica de Innovación*; (MinTIC, 2017b), y que muestra cómo la ciberseguridad (ciberespacio, seguridad informática y ciberdefensa, entre otros) se ha convertido en un eje estratégico y prioritario para proteger los recursos y activos informáticos de la nación.

Igualmente, a través de la política de gobierno digital y el programa de gobierno en línea (Gobierno de Colombia, 2018), el Estado ha diseñado políticas, procedimientos, monitoreo y asistencia técnica para fortalecer los temas de ciberseguridad y ciberdefensa,

usando parámetros y modelos que propenden por la confidencialidad, la integridad y la disponibilidad de los datos.

En cuanto a la detección de riesgos cibernéticos, dada la complejidad tecnológica asociada y la gran variedad de entidades que conforman el estado, se vienen desarrollando modelos de riesgos para la detección y análisis de amenazas y vulnerabilidades en sus sistemas de información para apoyar la prevención, protección y detección temprana de incidentes cibernéticos. Asimismo, el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa, la Policía y ColCERT (Colcert, s.f.)[3] vienen desarrollando esquemas de perfilación, monitoreo y control de la infraestructura crítica del país que puede estar expuesta a ataques cibernéticos que pueden llevar a catástrofes para la nación y afectar su soberanía. En el mismo sentido, en abril de 2016 se creó el Cibergaula (Policía Nacional de Colombia, 2018), para contrarrestar delitos de ciberextorsión, y desde 2018 se generó el Computer Security Incident Response Team (CSIRT), conformado por la Policía, Colcert y MinTIC, para prevenir y responder a los ataques informáticos dirigidos a entidades públicas.

A pesar de ello, aún se carece de un número suficiente de expertos en la temática que permita seguir avanzando al ritmo en que el cibercrimen se viene desarrollando y sin que exista una tendencia en procesos de formación que esté acompañando el proceso. En el ámbito académico (SNIES) solo se encuentra la Maestría en Ciberseguridad y Ciberdefensa (Ministerio de Educación Nacional, 2017) que se desarrolla con alianza entre la Escuela Superior de Guerra (s.f.) y el MinTIC. Lo mismo ocurre en la educación para el trabajo y el desarrollo humano (educación no formal), en donde hasta el año 2018, existía escasa oferta de diplomados y cursos sobre este tema, exceptuando el Diplomado en Ciberseguridad y Ciberdefensa que oferta la misma Esdegue. Gracias a la realidad descrita es que en los útimos años se ha venido ampliando significativamente la oferta, como es el caso del Diplomado de Ciberseguridad y Cultura Cibernética de la UMNG y otros programas relacionados, en diversas universidades del país. No obstante, al respecto tendrían que considerarse aspectos curriculares y educativos para la formación sobre la temática (Cayón y García, 2014).

Todo esto muestra la magnitud de este fenómeno, sus múltiples manifestaciones y la vulnerabilidad existente en el país, que ha elevado el nivel de riesgo existente en función de los nefastos impactos que se pueden generar para ciudadanos y organizaciones.

3. Estas entidades realizan la coordinación de las acciones necesarias para la protección de la infraestructura crítica del estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacionales.

Sistemas de gestión y normas de ciberseguridad en Colombia

En cuanto a los sistemas de gestión, el MinTIC publicó el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la estrategia GEL, a saber: TIC para servicios, TIC para gobierno abierto y TIC para gestión (MinTIC, s.f.).

Este modelo toma como base las buenas prácticas de seguridad de la ISO 27001 de 2013 y la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, y pretende preservar la confidencialidad, integridad y disponibilidad de los activos de información, garantizar el buen uso y privacidad de los datos, contribuir con la transparencia en la gestión y promover el uso de las mejores prácticas de seguridad de la información en las entidades públicas (como base de la seguridad digital).

De esta forma, el MSPI constituye la base de la estrategia de gobierno digital impulsado por el Estado y que se ha hecho obligatoria para todas las entidades públicas de orden nacional y territorial, por lo que se estableció el 2020 como plazo para su implementación general, buscando construir un Estado más eficiente, transparente y participativo (MinTIC, s.f.). Unido a esto, se encuentra la Política de Seguridad Digital del MIPG.

Por otra parte, teniendo en cuenta la grave situación de cibercrimen en el contexto global, y dado el alto grado de vulnerabilidad de Colombia en torno a los delitos informáticos, el país también ha tenido que ir trabajando en la generación de políticas, marcos normativos, actos administrativos y otras figuras jurídicas que incorporan los delitos informáticos en la legislación para fortalecer los procesos jurídicos, constitucionales, penales y sancionatorios frente al tema, con lo cual se ha logrado ya un marco jurídico amplio al respecto (Tabla 4).

Un ejemplo de este paquete de normas se encuentra en el documento Conpes 3701 (DNP, 2017) que establece los *Lineamientos de política para ciberseguridad y ciberdefensa* en Colombia y constituye el principal referente y derrotero de la política pública en función de desarrollar una estrategia nacional que evite y contrarreste las amenazas informáticas que puedan afectar significativamente al país hacia el futuro, entendiendo la ciberseguridad como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética (MinTIC, 2017c). Como complemento, se encuentra el Conpes 3854 (DNP, 2016) en el cual se establece la Política Nacional de Seguridad Digital.

Tabla 4.
Marco normativo sobre ciberseguridad en Colombia

Normatividad	Descripción
Ley 527	Acceso y uso de mensajes de datos, comercio electrónico y firmas digitales, y determinación de entes certificadores (Congreso de la República de Colombia, 1999).
Ley 594	Seguridad de archivos (Congreso de la República de Colombia, 2000a).
Ley 599	Violación ilícita de comunicaciones, derechos de autor y algunos delitos informáticos en el Código Penal (Congreso de la República de Colombia, 2000b).
Ley 679	Prevención y ataque contra la explotación, la pornografía y el turismo sexual con menores (Congreso de la República de Colombia, 2001).
Ley 962	Reducción de trámites y procedimientos administrativos de entidades públicas o privadas con funciones públicas o de servicios públicos (Congreso de la República de Colombia, 2005).
Ley 1266	*Habeas data* y manejo de información de bases de datos personales (Congreso de la República de Colombia, 2008).
Ley 1273	Modificación del Código Penal para acoger la protección de la información y la preservación integral de los sistemas que usan TIC (Congreso de la República de Colombia, 2009a).
Ley 1341	Principios y conceptos sobre la sociedad de la información y la organización de las TIC y creación de la Agencia Nacional del Espectro (Congreso de la República de Colombia, 2009b).
Ley 1437	Pruebas electrónicas para tipificar los delitos en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo (Congreso de la República de Colombia, 2011a).
Ley 1480	Protección al consumidor por medios electrónicos y seguridad en transacciones electrónicas en el Estatuto del Consumidor (Congreso de la República de Colombia, 2011b).
Decreto-Ley 019	Reducción de trámites en el estado a través de medios electrónicos y establecimiento de criterios de seguridad (Presidencia de la República de Colombia, 2012a).
Decreto 2693	Estrategia de gobierno electrónico (Presidencia de la República de Colombia, 2012b).
Decreto 2364	Posibilidad de la firma electrónica (Presidencia de la República de Colombia, 2012c).
Decreto 2609	Posibilidad del expediente electrónico en el esquema de gestión documental estatal (Presidencia de la República de Colombia, 2012d).
Ley 1581	Regulación de la protección de datos personales de los individuos (Congreso, 2012).
Ley Estatutaria 1621	Normatividad para las labores de Inteligencia y contrainteligencia y criterios de seguridad para este rol (Congreso de la República de Colombia, 2013).
Decreto 1377	Reglamentación de la la protección de datos personales de los individuos (Presidencia de la República de Colombia, 2013a).
Decreto 1510	Contratación y compra pública por medios electrónicos (Presidencia de la República de Colombia, 2013b).
Ley 1712	Criterio de transparencia en el acceso a la información pública (Congreso de la República de Colombia, 2014).
Decreto 333	Determinación de las entidades de certificación digital (Presidencia de la República de Colombia, 2014).
Ley 1978	Modernización del sector de las tecnologías de la información y las comunicaciones (Congreso de la República de Colombia, 2019).
Decreto 620	Lineamientos generales en el uso y operación de los servicios ciudadanos digitales (Presidencia de la República de Colombia, 2020).
Conpes 3975	Política Nacional para la transformación digital e inteligencia artificial (DNP, 2019).

Fuente: elaboración propia.

Se observa ya una amplia legislación en el país y avances importantes en torno a la ciberseguridad, aunque esto no ha logrado contrarrestar suficientemente las diversas modalidades de delitos informáticos existentes pues, por el contrario, se observa su crecimiento, variación y rápida evolución, sobre todo porque estos se encuentran en manos de grandes empresas criminales organizadas que terminan generando enormes perjuicios económicos y sociales.

Conclusiones

El análisis realizado muestra que, a pesar de los esfuerzos realizados, Colombia presenta importantes vulnerabilidades ante las amenazas cibernéticas. Esto se evidenció claramente en 2020 con el aumento de las interacciones mediadas por internet y otras TIC, derivado del aislamiento preventivo decretado para enfrentar la pandemia (COVID-19) y que generó un

aumento significativo en los delitos cibernéticos contra Estados, organizaciones y personas.

En consecuencia, se hace necesario promover en el país sólidas políticas de seguridad que protejan la información de personas y diversas organizaciones y que incorporen las reglas y procedimientos para la gestión de la información, la protección física de los equipos en red, la determinación de barreras y procesos de acceso a datos y el establecimiento de los niveles de acceso de acuerdo con responsabilidades y funciones, la limitación de acceso a terceros, los reportes de intrusión, los estándares de seguridad, la codificación de información, el uso de software legal, el uso de protecciones ante ataques externos, los *backups* de información y la revisión de adjuntos en mensajería, entre otros.

También se requiere mejorar los esquemas para el análisis y la medición automatizada, continua y en tiempo real de los riesgos, amenazas y vulnerabilidades existentes en los sistemas de información gubernamental (mapas de riesgo), para decidir y actuar en prevención, protección y detección temprana de incidentes cibernéticos. Se requiere entonces diseñar y actualizar las políticas y acciones tendientes a minimizar los riesgos asociados a las amenazas cibernéticas que puedan afectar la nación, la sociedad, las organizaciones y los individuos.

Dado que este tema constituye un problema de índole mundial, se considera importante que el Estado colombiano consolide alianzas y desarrolle estrategias de cooperación internacional que le permitan aumentar los estándares de ciberseguridad y enfrentar conjuntamente las amenazas cibernéticas y proteger su infraestructura crítica, particularmente en el contexto latinoamericano (Izycki, 2018), considerando tanto la soberanía como la interdependencia (Saavedra y Parraguez, 2018a).

El gobierno debe seguir trabajando en estrategias que involucren a las entidades estatales, empresas, hogares, etc., para "blindar" el ciberespacio nacional frente a las potenciales amenazas. Como complemento, las diversas organizaciones del país deben promover y financiar la implementación de los SGSI, incluyendo la ISO 27001, para que los riesgos cibernéticos sean conocidos, asumidos, gestionados y reducidos y para que sus prácticas de protección se hagan más seguras y eficientes, pues el número de certificaciones es realmente bajo.

Igualmente, se deben fortalecer el MSPI y la Política de Seguridad Digital en el país, como referentes para todas las organizaciones y como pilar de la estrategia de Gobierno Digital que enmarca y debería estar presente en todas las entidades públicas en 2020, socializar el contenido de los Conpes 3701 y 3854 y facilitar su implementación para construir y consolidar una estrategia nacional frente a las amenazas informáticas que podrían afectarlo significativamente.

También se requiere promover y apoyar la investigación, desarrollo e innovación (I+D+i) sobre ciberseguridad, en función de generar conocimientos y soluciones de alto nivel, y desarrollar programas de educación formal (pregrados y posgrados) y de educación no formal (cursos, seminarios, diplomados, etc.) que preparen a los profesionales requeridos para trabajar en ciberseguridad en las diversas organizaciones, con competencias para generar conceptos y procedimientos propios y para analizar holísticamente los casos en el marco legislativo existente, en función de contrarrestar la ciberdelincuencia.

El Estado también debe generar mayores estrategias y acciones para la protección eficiente de la infraestructura crítica, de los sistemas de soporte operacional, de los procesos, de las plataformas de atención al ciudadano y del ciberespacio, que concuerden con la política de seguridad de la información e informar, capacitar y formar ampliamente a sus funcionarios y ciudadanos en ciberseguridad, dado que las personas resultan ser el eslabón más débil en la cadena de protección. En este sentido, el gobierno debe desarrollar consistentemente una estrategia y plan de comunicaciones sobre el tema, segmentando los destinatarios y precisando el mensaje institucional, que favorezcan las buenas prácticas en ciberseguridad, sobre todo frente al sector público (Ospina, 2020).

Finalmente, se debe fomentar la denuncia de delitos cibernéticos para poder determinar la magnitud real del fenómeno y los frentes prioritarios de acción y como apoyo a la gestión de las autoridades encargadas y avanzar rápidamente en términos legislativos para lograr la penalización de los delitos informáticos, que sí evolucionan rápidamente.

Referencias

Amador, M. (1998). *Redes telemáticas y educación*. Máster en Multimedia y Educación, Sevilla.

Amato, F., Castiglione, A., De Santo, A., Moscato, V., Picariello, A., Persia, F., Sperlí, G. (2018). Recognizing human behaviours in online social networks. *Computers and Security*, 74, 355-370. https://doi.org/10.1016/j.cose.2017.06.002

Barrett, M. P. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. Gaithersburg, Maryland (USA): National Institute of Standards and Technology - U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

BBC Noticias. (2017). Un nuevo ciberataque de gran escala afecta a compañías e instituciones de todo el mundo. Recuperado el 30 de julio

de 2017 de http://www.bbc.com/mundo/noticias-internacional-40422053

Cano, J. (2011). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. *Sistemas*, 119, 4-7. http://52.0.140.184/typo43/fileadmin/Revista_119/Editorial.pdf

Cayón, J., y García, L.A. (2014). La importancia del componente educativo en toda estrategia de Ciberseguridad. *Estudios en seguridad y defensa*, 9(18), 5-13. https://doi.org/10.25062/1900-8325.9

Clarke, R.A. y Knake, R.K. (2011). *Guerra en la red, los nuevos campos de batalla*. Barcelona: Editorial Planeta.

Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) (2017). Alertas de seguridad. Recuperado el 12 de octubre de 2017 de http://www.colcert.gov.co/

Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) (s.f.).Acerca de Colcert. Recuperado el 12 de octubre de 2017 de http://www.colcert.gov.co/?q=acerca-de

Congreso de la República de Colombia. (1999). *Ley 527 de 1999: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones*. Bogotá D.C.: Diario Oficial.

Congreso de la República de Colombia. (2000a). *Ley 594 de 2000: Por medio de la cual se dicta la Ley General de Archivos - Criterios de Seguridad y se dictan otras disposiciones*. Bogotá D.C.: Diario Oficial.

Congreso de la República de Colombia. (2000b). *Ley 599 de 2000: Por la cual se expide el Código Penal*. En esta se mantuvo la estructura del tipo penal de violación ilícita de comunicaciones, se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático. Bogotá D.C.: Diario Oficial.

Congreso de la República de Colombia. (2001). *Ley 679 de 2001: Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores*. Bogotá D.C.: Diario Oficial.

Congreso de la República de Colombia. (2005). *Ley 962 de 2005: Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos*. Bogotá D.C.: Diario Oficial.

Congreso de la República de Colombia. (2008a). *Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones*. Bogotá D.C.: Diario Oficial.

Congreso de la República de Colombia. (2008b). *Ley 1341 de 2009: Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones*. Bogotá D.C.: Diario Oficial.

Congreso de la República de Colombia. (2009a). *Ley 1273 de 2009: 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 comunicaciones, entre otras disposiciones*. Bogotá D.C.: Diario Oficial.

Congreso de la República de Colombia. (2011a). *Ley 1437 de 2011: Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo*. Bogotá D.C.: Diario Oficial.

Congreso de la República de Colombia. (2011b). *Ley 1480 de 2011: Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones*. Bogotá D.C.: Diario Oficial.

Congreso de la República de Colombia (2012). *Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales*. Bogotá D.C.: Diario Oficial.

Congreso de la República de Colombia (2013). *Ley Estatutaria 1621 de 2013: Por medio del cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal*. Bogotá D.C.: Diario Oficial.

Congreso de la República de Colombia (2014). *Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones*. Bogotá D.C.: Diario Oficial.

Datasec (s.f.). Certificados ISO/IEC 27001 emitidos a nivel mundial. Recuperado el 2 de julio de 2017 de http://www.datasec.com.uy/es/blog/certificados-isoiec-27001-emitidos-nivel-mundial

Departamento Administrativo de la Función Pública (DAFP). (2018). Resultados de la consulta FURAG para el año 2018 por sector. Recuperado el 24 de julio de 2019 de https://www.funcionpublica.gov.co/web/mipg/resultados-2018

Departamento Nacional de Planeación (DNP). (2016). Documento Conpes 3854: política nacional de seguridad digital. Recuperado el 9 de octubre de 2017 de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Departamento Nacional de Planeación (DNP). (2017). Documento Conpes 3701: lineamientos de política para ciberseguridad y ciberdefensa. Recuperado el 5 de mayo de 2017 de https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Departamento Nacional de Planeación (DNP). (2019). Política Nacional para la transformación digital e inteligencia artificial. Recuperado el 2 de diciembre de 2019 de https://www.mintic.gov.co/portal/604/articles-107147_recurso_1.pdf

Ekman, E. (1989). *La documentación en investigación educativa. En: T. Husén y N. Postlethwaite (eds.), Enciclopedia Internacional de la Educación*. Barcelona: Vicens-Vives/MEC.

El Diario. (2017). ¿La Primera Ciberguerra Mundial? Recuperado el 22 de julio de 2017 de http://www.eldiario.es/cultura/tecnologia/Primera-Ciberguerra-Mundial_0_598790464.html

El Heraldo. (2017). Ciberataque golpeó a 11 empresas y una entidad pública en Colombia. Recuperado el 20 de mayo de 2017 de https://www.elheraldo.co/ciencia-y-tecnologia/ciberataque-golpeo-11-empresas-y-una-entidad-publica-en-colombia-361747

ElTiempo. (2017). En Colombia hay 12 empresas afectadas por ciberataque mundial. Recuperado el 12 de noviembre de 2020 de http://www.eltiempo.com/tecnosfera/novedades-tecnologia/numero-de-empresas-afectadas-en-colombia-por-ciberataque-mundial-103550

El Tiempo. (2018). Ciberseguridad y ciberdefensa, temas claves de cita de Duque con Otán. Recuperado el 28 de mayo de 2020 de https://www.eltiempo.com/politica/gobierno/los-temas-claves-de-cita-de-duque-con-el-secretario-general-de-la-otan-284598

El Tiempo. (2019). En 2019 se reportaron más de 28.000 casos de ciberataques en Colombia. Recuperado el 19 de enero de 2020 de https://www.eltiempo.com/tecnosfera/novedades-tecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790

El Tiempo. (2020). Hurto informático: 'Con una sola llamada me robaron mis ahorros'. Recuperado el 23 de abril de 2020 de https://www.eltiempo.com/justicia/servicios/coranavirus-fraude-bancario-le-robaron-sus-ahorros-con-una-llamada-487340?utm_medium=Social&utm_source=Facebook&fbclid=IwAR3wH6tAP27lx-ji-fpcIMRWoGfG_CXnt6JkMOuJaUCod6B7vu4n4vW11yI#Echobox=1587656034

El Universal (2020). Venden cuentas Zoom en la dark web. Recuperado el 10 de julio de 2020 de https://www.eluniversal.com.mx/techbit/millones-de-cuentas-de-zoom-se-venden-en-la-dark-web

El Universal (2020). Hackean a Bill Gates, lo acusan de haber creado el coronavirus. Recuperado el 23 de abril de 2020 de https://www.eluniversal.com.mx/techbit/hackean-bill-gates-lo-acusan-de-haber-creado-al-coronavirus

Escuela Superior de Guerra (ESDEGUE). (s.f.). Maestría en Ciberseguridad y ciberdefensa. Recuperado el 26 de octubre de 2017 de https://ciber.esdegue.edu.co/

Eslava, H., Rojas, L.A., y Pineda, D. (2013). Cybersecurity recommendations for communication systems in the colombian electrical sector. Paper presented at the IET Conference Publications, 2013 (615 CP). https://doi.org/10.1049/cp.2013.0538

European Parliament y Council of the European Union. (2016). Regulation (EU) 2016/679: on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); General Data Protection Regulation (EU) - GDPR-. Official Journal of the European Union. Bruselas.

Gaitán, A. (2014). *El ciberespacio, un nuevo teatro de batalla para los conflictos armados del siglo XXI*. Bogotá: Escuela Superior de Guerra.

Gobierno de la República de Colombia (2019). Conoce la política de Gobierno en línea. Recuperado el 20 de febrero de 2019 de http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7650.html

Hatfield, J.M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers and Security*, 73, 102-113. https://doi.org/10.1016/j.cose.2017.10.008

Henriques, A.P., Silva, M.M., Poleto, T., Camara, L., & Cabral, A.P. (2018). Cybersecurity risk analysis model using fault tree analysis and

fuzzy decision theory. *International Journal of Information Managemen*t, 43, 248-260. https://doi.org/10.1016/j.ijinfomgt.2018.08.008

Hernández, I. (2002). *La investigación científica: Un camino a la imaginación*. Bogotá: Universidad Piloto de Colombia.

Hernández, J. C. (2018). Estrategias Nacionales de Ciberseguridad en América Latina. *Grupo de Estudios en Seguridad Internacional (GESI)*, 8, 5 p. Recuperado el 2 de mayo de 2019 de http://www.seguridadinternacional.es/?q=es/print/1335.

IBM. (2018). Estudio anual Cyber Resilient Organization. Recuperado el 26 de Agosto de 2019 de https://www.ibm.com/blogs/transformacion/2018/03/21/nuevo-estudio-ponemon-demasiadas-organizaciones-plan-responder-ante-incidentes/

Incibe. (s.f.). Protección de la información. Recuperado el 28 de noviembre de 2017 de https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-informacion

International Standards Organization (ISO). (2005). *ISO 27000: Sistema de Gestión de la Seguridad de la Información*. Recuperado el 14 de agosto de 2017 de http://www.iso27000.es/download/doc_iso27000_all.pdf

International Standards Organization (ISO). (2018). *ISO 27000: Sistema de Gestión de la Seguridad de la Información*. Recuperado el 14 de agosto de 2017 de http://www.iso27000.es/download/doc_iso27000_all.pdf

International Telecommunication Union (ITU). (2010). Unión Internacional de Telecomunicaciones. Recuperado el 10 de octubre de 2016 de http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

International Telecommunication Union (ITU). (2017). Global Cybersecurity Index (GCI). Recuperado el 12 de mayo de 2018 de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

International Telecommunication Union (ITU). (2018). Guide to developing a national cybersecurity strategy: Strategic engagement in cybersecurity. Génova (Suiza): International Telecommunication Union -ITU-, the World Bank, Commonwealth Secretariat -ComSec-, the Commonwealth Telecommunications Organisation -CTO-, NATO Cooperative Cyber Defence Centre of Excellence -NATO CCD COE- y -IGOs-.

Izycki, E. (2018). National cyber security strategies in Latin America: Opportunities for convergence of interests and consensus building. RISTI - Revista Ibérica de Sistemas e Tecnologías de Informacao, (E15), 39-52.

Jordan, A., y Dixon, W. (2018). ¿Por qué la cuarta revolución industrial necesita más graduados en carreras humanísticas? World Economic Forum. Recuperado el 3 de enero de 2019 de https://es.weforum.org/agenda/2018/12/por-que-la-cuarta-revolucion-industrial-necesita-mas-graduados-en-carreras-humanisticas/

Koch, S. (2015). La libertad en el ciberespacio: ciberseguridad y el principio del daño. *Revista Ensayos Militares*, 1(2), 85-98.

Marín, J., Nieto, Y., Huertas, F., y Montenegro, C. (2019). Ontological model of cybercrimes: Case study Colombia [Modelo ontológico de los ciberdelitos: Caso de estudio Colombia. *RISTI - Revista Ibérica de Sistemas* e *Tecnologías de Informacao*, (E17), 244-257.

Mertens, D. M. (2010). Research and evaluation in education and psychology: Integrating diversity with quantitative, qualitative, and mixed methods (3 ed.). Thousand Oaks (California): Sage.

Ministerio de Educación Nacional. (2017). Módulo de consultas del Sistema Nacional de Información de la Educación Superior -SNIES-. Recuperado el 18 de julio de 2017 de https://snies.mineducacion.gov.co/consultasnies/programa#

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (s.f.). Sistemas de Gestión de la Seguridad de la Información (SGSI). Recuperado el 2 de agosto de 2017 de http://www.mintic.gov.co/gestionti/615/w3-article-5482.html

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (s.f.). Modelo de Seguridad y Privacidad de la Información. Recuperado el 2 de noviembre de 2017 de https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2017a). Suscriptores de internet. Recuperado el 18 de julio de 2017 de http://colombiatic.mintic.gov.co/679/w3-propertyvalue-47275.html

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2017b). Ciberseguridad. Recuperado el 5 de julio de 2017 de http://www.mintic.gov.co/portal/604/w3-article-6120.html

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2017c). Agenda estratégica de innovación: ciberseguridad. Recuperado el 1 de octubre de 2017 de http://www.mintic.gov.co/portal/604/articles-6120_recurso_2.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2017d). Impactos de los incidentes de seguridad digital en Colombia 2017. Recuperado el 28 de agosto de 2018 de https://www.oas.org/documents/spa/press/Estudio-Seguridad-Digital-Colombia.pdf

Noticiero CM&. (2020). Aumenta hackeo a empresas ante expansión de teletrabajo. Recuperado el 23 de abril de 2020 de https://noticias.canal1.com.co/internacional/aumenta-hackeo-por-teletrabajo/?fbclid=IwAR0bKZR7wllOtdRZz93xmzCmYoKee5EdY4SCLRoRMLH2z-5dLF-lo7sEr4g

Organization for Economic Cooperation and Development (OECD). (2019). Policies for the protection of critical information infrastructure: Ten years later. París: OECD Publishing.

Oppenheimer, A. (2018). *¡Sálvese quien pueda! El futuro del trabajo en la era de la automatización*. Bogotá, D.C.: Debate.

Ospina, M. R. (2020). *Marketing Público.* Bogotá: Klasse Editorial.

Osorio, A. (2017). Ciberseguridad y ciberdefensa: Pilares fundamentales de la seguridad y defensa nacional. *Revista Fuerzas Armadas*, 90(241), 6-14.

Policía Nacional de la República de Colombia. (2017a). Informe: Balance Cibercrimen en Colombia 2017. Recuperado el 19 de noviembre de 2017 de https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf

Policía Nacional de la República de Colombia. (2017b). Informe: Amenazas del Cibercrimen en Colombia 2016-2017. Recuperado el 1/6/2017 de https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Policía Nacional de la República de Colombia. (2017c). Ciberseguridad. Recuperado el 8 de agosto de 2017 de https://www.policia.gov.co/ciberseguridad

Policía Nacional de la República de Colombia. (2017d). Informe: Costos del cibercrimen en Colombia (2016-2017). Recuperado el 19 de enero de 2020 de https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

Policía Nacional de la República de Colombia (2018). Cibergaula - Dirección Antisecuestro y Antiextorsión de la Policía Nacional de Colombia. Recuperado el 12 de julio de 2018 de https://www.policia.gov.co/direcciones/antisecuestro

Policía Nacional de la República de Colombia. (2019). Informe: Tendencias del Cibercrimen Colombia (2019-2020). Recuperado el 26 de diciembre de 2019 de https://caivirtual.policia.gov.co/#observatorio

Powerdata (2019). GDPR: Lo que debes saber sobre el reglamento general de protección de datos. España: Grupo PowerData. Recuperado el 26/8/2019 de https://www.powerdata.es/gdpr-proteccion-datos

Presidencia de la República de Colombia. (2012a). *Decreto - Ley 019 de 2012: Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública*. Bogotá D.C.: Diario Oficial.

Presidencia de la República de Colombia. (2012b). *Decreto 2693 de 2012: Por el cual se establecen los lineamientos generales de la estrategia de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones*. Bogotá D.C.: Diario Oficial.

Presidencia de la República de Colombia. (2012c). *Decreto 2364 de 2012: Por medio del cual se reglamenta el artículo de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones*. Bogotá D.C.: Diario Oficial.

Presidencia de la República de Colombia. (2012d). *Decreto 2609 de 2012: Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado*. Bogotá D.C.: Diario Oficial.

Presidencia de la República de Colombia. (2013a). *Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012*. Bogotá D.C.: Diario Oficial.

Presidencia de la República de Colombia. (2013b). *Decreto 1510 de 2013: Por el cual se reglamenta el sistema de compras y contratación pública*. Bogotá D.C.: Diario Oficial.

Presidencia de la República de Colombia. (2014). *Decreto 333 de 2014: Por el cual se reglamenta el artículo 160 del Decreto-ley 19 de 2012*. Bogotá D.C.: Diario Oficial.

Reyna, D., y Olivera, D.A. (2017). *Las amenazas cibernéticas*. (pp. 49-72). En Carlos Hernández Rodríguez y Raúl Manuel Arano Chávez. 10 Temas de Ciberseguridad. Veracruz, México: Editorial Universidad de Xalapa.

Revista Dinero (2016). El 43% de las empresas colombianas no están preparadas contra los ciberataques. Recuperado el 18 de mayo de 2017 de http://www.dinero.com/pais/articulo/colombia-tuvo-perdidas-de-1-billon-por-ciberataques/224404

Revista Semana (2020). EEUU ordena cierre de consulado chino en Houston. Consultado el 23 de julio de 2020 de https://www.semana.com/mundo/articulo/eeuu-ordena-cierre-de-consulado-chino-en-houston-noticias-del-mundo/688036

Saavedra, B., y Parraguez, L. (2018a). La ciberseguridad: análisis político y estratégico I. *Revista Fuerzas Armadas*, 91(243), 44-51.

Saavedra, B., y Parraguez, L. (2018b). La ciberseguridad: análisis político y estratégico II. *Revista Fuerzas Armadas*, 91(244-245), 73-80.

Sanabria, P. E. (2016). *Investigación en ciencias sociales y de gestión: Guía para el desarrollo de marcos metodológicos y procesos de investigación* (Working Paper). Bogotá D.C.: Universidad Militar Nueva Granada.

Sawyer, B.D., y Hancock, P.A. (2018). Hacking the Human: The Prevalence Paradox in Cybersecurity. *Human Factors*, 60(5), 597-609. https://doi.org/10.1177/0018720818780472

Stevens, T. (2018). Cyberweapons: Power and the governance of the invisible. *International Politics*, 55(3-4), 482-502. https://doi.org/10.1057/s41311-017-0088-y

Sutton, A.H. (2016). La pregunta de investigación en los estudios cualitativos. *Investigación en Educación Médica*, 5(17), 49-54. https://doi.org/10.1016/j.riem.2015.08.008

Telesur (2016). WikiLeaks revela que Panamá Papers fue financiado por EEUU. Recuperado el 12 de enero de 2017 de https://www.telesurtv.net/news/WikiLeaks-revela-que-Panama-Papers-fue-financiado-por-EE.UU.-20160406-0013.html

RED+. (2019). Duplican perfiles de Facebook para estafar usuarios. Recuperado el 26 de julio de 2019 de http://www.redmas.com.co/colombia/duplican-perfiles-de-facebook-para-estafar-usuarios/

Tamayo, M.T. (2011). *El proceso de la investigación científica*. México: Limusa.

WikiLeaks. (2015). What is WikiLeaks. Recuperado el 4 de septiembre de 2017 de https://wikileaks.org/What-is-WikiLeaks.html

Vanguardia (2019). Hurtos informáticos delincuentes invisibles. Recuperado el 2 de febrero de 2019 de https://www.vanguardia.com/colombia/hurtos-informaticos-delincuentes-invisibles-xg1338198