Estrategia Jurídica para la Gestión, Análisis y Ciberseguridad de la Información en la Investigación Penal

Marco Emilio Sánchez Acevedo

Trabajo de grado para optar al título profesional:

Maestría en Ciberseguridad y Ciberdefensa

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

2018

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
ESCUELA SUPERIOR DE GUERRA
PROGRAMA MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA NACIONAL

ESTRATEGIA JURÍDICA PARA LA GESTIÓN, ANÁLISIS Y CIBERSEGURIDAD DE LA INFORMACIÓN EN LA INVESTIGACIÓN PENAL

MARCO EMILIO SÁNCHEZ ACEVEDO

DIRECTOR
JULIÁN DAVID APONTE DÍAZ

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR EL TITULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA
BOGOTA – COLOMBIA
2018

Bogotá, 17 de octubre de 2017

A Dios, gracias por siempre.

A mis hijos y a mi esposa, son la luz en el camino,

a mis padres y hermanos,

al profesor Julián Aponte.

A todos, su tiempo fue mi tiempo.

Agradecimientos

Al Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, a la Escuela Superior de Guerra del Ministerio de Defensa Nacional, pues gracias a su apoyo he podido realizar y culminar con éxito este proceso académico. De la misma manera, un reconocimiento a la Fiscalía General de la Nación, pues el conocimiento y experiencia que me dio sirvieron de base para la estructuración de este proyecto. A la Fundación IN-NOVA que apostó a la creación de un programa único en la región.

Resumen

Cinco cuestiones se plantean a manera de discusión cuando se habla de una estrategia para la gestión, análisis y seguridad de la información en la investigación penal a partir del uso de Tecnologías de la Información y las Comunicaciones: la primera de ellas tiene que ver con la afectación a la cláusula de reserva que tienen las investigaciones en la fase inicial, esto es, en los procesos seguidos por la Ley 600 de 2000 en su etapa previa, ora en las investigaciones que se siguen por el procedimiento de Ley 906 de 2004 hasta la fase del descubrimiento probatorio; el segundo aspecto, que es susceptible de discusión, es el relacionado con el tratamiento de los datos personales de los ciudadanos incursos en las investigaciones criminales, puesto que su tratamiento no debe sobrepasar la esfera de la finalidad, vale decir, de la propia investigación criminal.

El tercer punto es el que atañe a la delimitación del instrumento jurídico a través del cual se incorporan a los procesos, como prueba, los resultados de los análisis objetivos, esto es, los contextos creados a partir del análisis de la información; la cuarta cuestión concierne a la garantía jurídica para la utilización de tecnologías en las investigaciones penales; y por último, se llega a la interrogante acerca de cuál debe ser la estrategia de ciberseguridad de la información en el marco del cumplimiento de la misión constitucional de la Fiscalía General de la Nación.

Por consiguiente, esta investigación aborda el planteamiento del problema a partir de la necesidad de generar una estrategia autónoma, independiente, pero armonizada e integrada, que responda a la pregunta planteada —y que a su vez incorpore una estrategia de ciberseguridad— dentro del ámbito de la realización de las actividades, excepcionales, administrativas que cumple la entidad.

Palabras clave: Análisis criminal, gobierno electrónico, investigación penal, *big data*, contexto, verdad, memoria, ciberseguridad.

Abstract

This paper present five questions appear like discussion about the strategy for the management, analysis and safety of the information in the penal investigation from the use of Technologies of the Information and the Communications: the first one of them has to see with the affectation to the clause of reservation that the investigations have in the initial phase, this is, in the processes followed by the Law 600 of 2000 in his previous stage, prays in the investigations that follow for the procedure of Law 906 of 2004 up to the phase of the evidential discovery; the second aspect, which is capable of discussion, is the related one to the treatment of the personal information of the private uncourses in the criminal investigations, Since his treatment must not exceed the sphere of the purpose, it is worth saying, of the own criminal investigation.

The third point is the one that concerns the delimiting of the juridical instrument across which there join to the processes, in proof, the results of the objective analyses, this is, the contexts created from the analysis of the information; the fourth question concerns the juridical guarantee for the utilization of technologies in the penal investigations; and finally, it comes near to the interrogante brings over of which it is necessary to do the cybersecurity strategy of the information in the frame of the fulfillment of the constitutional mission of the General District attorney's office of the Nation.

Consequently, this research approaches the exposition of the problem from the need to generate an autonomous, independent, but harmonized and integrated strategy, which answers to

the raised question (and that in turn incorporates a strategy of cybersecurity) inside the area of the accomplishment of the activities, exceptional, administrative that fulfills the entity.

Key words:

Criminal analysis, e-administration, Criminal investigation, big data, Public Law, truth, memory, cybersecurity.

Contenido

Índice de tablas

Índice de figuras

Tabla de abreviaturas

Capítulo	Cap.
Coordinador	Coord.
Edición	Ed.
Sin fecha	s.f.
Sin página	s.p.
Página (páginas)	p. (pp.)
Párrafo	párr.

Estrategia jurídica para la gestión, análisis y ciberseguridad de la información en la investigación penal

MARCO EMILIO SÁNCHEZ ACEVEDO
Alumno de la Maestría Ciberseguridad y Ciberdefensa Nacional
I cohorte, Escuela Superior de Guerra

Pregunta de investigación

¿Qué estrategia jurídica debe seguir la Fiscalía General de la Nación para la gestión, análisis y ciberseguridad de la información en la investigación penal cuando utiliza TIC?

Objetivo general

Generar una estrategia jurídica que propenda por la seguridad en la gestión y análisis de la información dentro de la investigación penal cuando se utilizan TIC, en especial sistemas de ciberseguridad.

Objetivos específicos

- Relacionar y estudiar las actividades de recolección, gestión y análisis de la información existentes en la Fiscalía General de la Nación (en adelante: FGN).
- Identificar y analizar la estructura de los sistemas de información que operan en la FGN, es decir, el Sistema Penal Oral Acusatorio (en adelante: SPOA), el Sistema de Información Judicial de la Fiscalía Ley 600 (en adelante: SIJUF) y el Sistema de Información de Justicia y Paz Ley 975 (en adelante: SIJYP).

- Analizar la estrategia de generación de contextos en el marco de las investigaciones y su vinculación con los sistemas de información misional (SPOA, SIJUF, SIJYP).
- Definir la estrategia de gestión, análisis y seguridad de la información para la FGN.

Metodología

En este documento se ha seguido la estrategia metodológica planteada por Taylor y Bogdan (1994). Por ello, se incluyen aspectos descriptivos y explicativos, y a partir del método inductivo se desarrollan las cuatro fases que componen el método: 1) codificación abierta de la información (organización inicial de la información); 2) codificación axial de la información (creación de un esquema conceptual a partir de la selección de los temas relevantes en el estudio y de la agrupación de la información); 3) codificación selectiva (delimitación de la teoría a partir del componente del marco teórico); 4) delimitación de la teoría emergente (formulación de una teoría con un grupo pequeño de conceptos de alta abstracción, delimitando la terminología y el texto propuesto).

1. Introducción: acercándose al estado de la cuestión

Desde un enfoque tradicional de la seguridad y defensa de los estados, el objetivo no es otro que repeler las amenazas que puedan llegar de actores militares estatales pertenecientes a otros Estados y que puedan poder en peligro los elementos esenciales del estado Territorio, soberanía y población nacional. Éste concepto trae consigo, que para hacer frente a las potenciales ofensas las fuerzas militares se dotan de capacidades que permitan enfrentar las amenazas. Éste planteamiento, en el siglo XXI, debe ser analizado y construido nuevamente, desde otros enfoques, que desde el entendimiento del significado de la sociedad de la información, incorpora nuevos retos.

Los Estados ya no son, solamente, territorio, soberanía y población, son actores del proceso dado por la globalización, existen, bajo esa condición, nuevas amenazas, nuevos riesgos que deben ser enfrentados, amenazas y riesgos que traspasan las fronteras tradicionales. Estados que no son únicos, sino que se relacionan con otros, personas de estados que actúan a nombre del estado o de forma independiente y por ende no representan la voluntad de un estado, sin embargo sus actos pueden generar consecuencias en el entorno internacional, el nuevo escenario plantea conceptos de necesario desarrollo como la identidad, las comunidades, las normas formas de poder, v.g. el de los datos, que deben ser afrontados y enfrentados de la innovación y la participación de múltiples partes interesadas[1].

[1] Un desarrollo de la Seguridad y defensa en Colombia, puede consultarse el "análisis comparado de las políticas creadas entre los años 2002 y 2012, Pablo Rivas Pardo, Revista Política y Estrategia, Nº. 120, 2012, págs. 57-77.

Aquel concepto de seguridad incorporado en la carta del Atlántico de 1941 y que fundamentó la Carta de las Naciones Unidas, en el numeral 8, debe trascender a la sociedad del siglo XXI, recuérdese que allí se señalaba:

> "(…)Puesto que ninguna paz futura puede ser mantenida si las armas terrestres, navales o aéreas continúan siendo empleadas por las naciones que la amenazan, o son susceptibles de amenazarla con agresiones fuera de sus fronteras, consideran que, en espera de poder establecer un sistema de seguridad general, amplio y permanente, el desarme de tales naciones es esencial. Igualmente ayudarán y fomentarán todo tipo de medidas prácticas que alivien el pesado fardo de los armamentos que abruma a los pueblos pacífcos (Carta del Atlántico, 1941).

Concepto que queda reflejado e impregnado en la Carta de las Naciones Unidas respecto a la "(…)la determinación de unir nuestras fuerzas para mantener la paz y la seguridad internacional(…)" (Carta de las Naciones Unidas, 1945).

La posterior llegada del concepto de seguridad colectiva indica un desarrollo normal del entendimiento de los cambios en el concepto tradicional, véase como el el Tratado del Atlántico Norte (OTAN) de 1949, señaló que "(…) la resolución de todos los gobiernos de unir sus esfuerzos en la defensa colectiva y en la conservación de la paz y la seguridad(…) se convertían en un elemento fundamental para enfrentar las nuevas amenazas, situación que también se refleja en los compromisos adquiridos con la firma de los Tratados del Sudeste Asiático (SEATO) de defensa colectiva de 1954, el Pacto de Varsovia de 1955, el Tratado Interamericano de Ayuda Recíproca

(TIAR) de 1948, la Resolución VIII la Conferencia Interamericana sobre Problemas de la Guerra y de la Paz, todos ellos con el ánimo de fianzas el concepto que la seguridad debe ser afrontada por el conjunto, pues las amenazas, en muchos casos son y corresponden a factores transversales.

En éste desarrollo natural, llega el concepto de seguridad multidimensional, acompañado por el desarrollo del mundo globalizado y fundamentado en la amenazas que dejan de ser tradicionales y la necesidad de innovar para hacer frente y así responder a las situaciones que se plantean en los nuevos escenarios, la llegada de nuevos actores internacionales, los nuevos mercados, los conceptos de nuevos ciudadanos, entre otros, no pueden enfrentarse de la forma en que se han enfrentado bajo la concepción de la seguridad y defensa nacional, los estados no tienen respuestas frente a estos escenarios, lo que lleva a plantear procesos de análisis desde las diversas ópticas y dimensiones, se llega a la necesidad de desarrollar nuevas investigaciones que den como resultado la delimitación de las nuevas amenazas (económicas, políticas, sociales, ambientales, entre otras), la definición de lo que significa una amenaza en el siglo de la sociedad de la información, las implicaciones que tienen estas nuevas amenazas en el entorno de los Derechos humanos de los ciudadanos y que trascienden al entorno de los Estados[2]. Es en este sentido que y dadas las magnitudes de los nuevos retos que se incorpora el concepto la Declaración de Seguridad sobre las Américas, celebrada en México en el año 2003, que trae conceptos de múltiples dimensiones como el ambiente, la seguridad humana, plantea amenazas emergentes como la

[2] Para la OEA el alcance multidimensional, incluye las amenazas tradicionales y las nuevas amenazas, preocupaciones y otros desafíos a la seguridad de los Estados del Hemisferio, incorpora las prioridades de cada Estado, contribuye a la consolidación de la paz, al desarrollo integral y a la justicia social, y se basa en valores democráticos, el respeto, la promoción y defensa de los Derechos Humanos, la solidaridad, la cooperación y el respeto a la soberanía nacional (OEA, 2003, Artículo II:2)

delincuencia transnacional, la exclusión social, los desastres naturales, la cibercriminalidad, son algunas de esos retos a ser enfrentados. La incorporación de civiles para hacer frente común a las nuevas amenazas que aunado a la llegada de la era de la información y la tecnología, debe entenderse, también, en el transito dimensión, de una física a una lógica, y cuyos actores, que son diversos, pueden ocasionar desestabilización[3].

Es precisamente desde el entendimiento de la nueva concepción de seguridad y defensa nacional y a partir de la materialización y desarrollo de la sociedad de la información, con la consecuente utilización de tecnologías de la información y las comunicaciones, que se plantea el objeto de estudio de éste trabajo. Una de las cuestiones a tratarse en las investigaciones criminales del siglo XXI es la que incorpora los elementos tecnológicos, sus retos y por sobre todo, la forma en que las propias tecnologías sirvan como canal para la materialización de la justicia.

Esta primera parte tiene como finalidad sentar las bases, a partir del estado del arte, de lo que significa el uso de tecnologías de la información y las comunicaciones en la investigación penal y, en consecuencia, construir una estrategia jurídica para la gestión, análisis y ciberseguridad de la información que se produce en dicho campo del derecho.

Desde la década de 1970 se han incorporado nuevos medios tecnológicos a las organizaciones públicas y privadas de Colombia; esto ha llevado a poner una "*e*" delante de sus nombres, dando lugar a términos como *e-administración, e-firma, e-justicia* o *e-democracia*. Se

[3] Al respecto véase el documento Seguridad y Defensa: conceptos en constante transformación de Carlos Enrique Álvarez y otros, en Escenarios y Desafíos de la Seguridad Multidimensional , ESDEGUE, 2017. Disponible en https://esdeguelibros.edu.co/index.php/editorial/catalog/book/27

trata de subrayar el instrumento electrónico sin modificar en lo demás la noción que sirve de base (Gascón, 2010).

La e-justicia es un ámbito específico del *e-government* (gobierno electrónico) y, por lo tanto, de las investigaciones electrónicas; es importante decir que aquella alude a la administración de justicia, la cual involucra los elementos personales y materiales al servicio de la adecuada gestión de este servicio público; por ello, su concepto y regulación quedan muy vinculados a los de e-administración e *e-government*.

En términos similares a la doctrina de Delgado García y Oliver Cuello (2006) y de Gascón I. (2010), la Comisión Europea definió la e-justicia como:

> [...] el recurso a las tecnologías de la información y la comunicación para mejorar el acceso de los ciudadanos a la justicia y para la eficacia de la acción judicial entendida como toda actividad consistente en resolver un litigio o sancionar penalmente una conducta. (2008, p. 3)

En ese orden de ideas, debo referir que la función principal de la Fiscalía General de la Nación (en adelante: FGN) es investigar las conductas que revistan la característica de delito (conductas típicas), y para el cumplimiento de este objetivo utiliza diversas herramientas tecnológicas: desde programas de gestión hasta aplicaciones específicas, pasando por herramientas individuales, como memorias USB, CD, grabadoras, discos duros, entre otros.

Para cada uno de los sistemas normativos aplicables, como la Ley 600 de 2000, Ley 975 de 2005 y Ley 906 de 2004, se manejan unas u otras herramientas tecnológicas, por lo cual las investigaciones pasan por situaciones como estas:

Se llevan en papel —además de los registros propios de los sistemas de información— y se incorporan para realizar las correspondientes acusaciones ante los jueces, respecto de los responsables, con un elemento adicional: al ser investigaciones penales, deben contar con un alto nivel de protección de la información.

Además, los diversos sistemas de información (SIJUF, SIJYP, SPOA) no son interoperables; por consiguiente, la información que existe entre unos y otros no se puede analizar ni gestionar. De hecho, en cuanto al estado actual de estos, el Plan Estratégico 2016-2020[4] del ente acusador —en su objetivo estratégico número 9, denominado Fortalecer la infraestructura tecnológica— afirma que:

> La FGN cuenta con varios sistemas de información misional que funcionan de forma dispersa y con poca comunicación entre ellos. Además, su principal sistema de gestión de casos (Sistema Penal Oral Acusatorio, SPOA) cumple once años de funcionamiento y con el tiempo ha tenido múltiples adiciones realizadas en su mayoría de forma inorgánica y desordenada. (FGN, 2016, p. 46, párr. 126)

En complemento con lo reseñado, el documento plantea en cuanto a la arquitectura institucional:

> [...] la FGN debe realizar un diagnóstico y formular un plan tecnológico a mediano plazo que le permita i) gestionar adecuadamente los procesos penales, ii) aplicar herramientas

[4] El Plan Estratégico 2016-2020 describe las prioridades de la FGN y establece la forma como estas se cumplirán en dicho cuatrienio. Expone los objetivos estratégicos, los principales proyectos y las metas de gestión y de resultado fijados para este periodo por el doctor Néstor Humberto Martínez Neira, Fiscal General de la Nación.

> vigorosas de análisis criminal y ii) tomar decisiones gerenciales y estratégicas con base en evidencia empírica sólida. Es necesario entonces definir e implementar una arquitectura institucional que le permita a la FGN alinear su operación con la tecnología requerida. (2016, párr. 127)

Así mismo, los sistemas de información existentes no incorporan la totalidad de la información de cada una de las carpetas de las investigaciones; entonces, puede decirse que son sistemas de gestión administrativa, pero no de análisis de información, ni mucho menos expedientes judiciales electrónicos.

Los datos físicos, de cada una de las carpetas, no se integran en su conjunto a los sistemas de información, y estos no realizan análisis para construir contextos y generar memoria; dichas deficiencias también fueron señaladas, en su momento, por la propia FGN en el informe de gestión para el periodo 2012 – 2016 (FGN, 2016b), aludiendo a un diagnóstico elaborado por la Universidad de los Andes en 2013:

> Una vez se asignan los casos al fiscal, no se percibieron políticas o lineamientos claros donde se implementen criterios de priorización, por lo que esta se encuentra sujeta a la autonomía de cada fiscal, en donde a veces se observa la iniciación de investigaciones que terminan siendo archivados, con el propósito de mejorar estadísticas propias en beneficio de la evaluación de desempeño personal del funcionario. Debido a lo anterior, algunos casos dejan de ser atendidos sin realizar un análisis adecuado, trayendo como consecuencia que la cantidad de aquellos que son archivados esté incrementando cada vez más. Universidad de los Andes (2013), citada por FGN (2016b, p. 30)

A lo anterior, se suma que no existe una estrategia jurídica normativa que señale altos estándares de ciberseguridad para la información que maneja la entidad.

Por otra parte, el transcurso del tiempo frente a la solución de las situaciones que se plantean a la justicia penal, así como las cifras de asuntos resueltos y hallazgo de los responsables es deficiente; en gran parte, esto se debe a la inexistencia de una estrategia para la gestión y el análisis de la información en el órgano de investigación.

La determinación de responsabilidades es un elemento esencial de la justicia, pero también lo es la necesidad de guardar la memoria y realizar investigaciones a partir de la delimitación de estructuras criminales, patrones de comportamiento, georreferenciación y construcción de contextos; esto solo es posible si la información allegada a las investigaciones se gestiona y se analiza.

Hoy en día, el Estado tiene el reto de incorporar las Tecnologías de la Información y la Comunicación (en adelante: TIC) para evitar el colapso de la administración de justicia. Las transformaciones del Estado contemporáneo exigen que estas tecnologías se involucren en las estructuras públicas como mecanismo de eficacia. Así, como afirma Cernada Badía (2012), este avance representa, más que una evolución, una revolución; toda vez que la *electronificación* del proceso judicial, y en particular de la investigación penal, no constituye un fin en sí mismo, sino un medio para mejorar el estándar de garantías que el ordenamiento jurídico impone al ejercicio de la función jurisdiccional.

1.1. Cómo se ha tratado este problema hasta ahora

El objetivo de este apartado es determinar la forma como ha sido abordado el tema, el avance de su conocimiento en el momento de realizar la presente investigación, y observar las

tendencias que existen. Como lo señala Vargas Guillén (1999), para realizar una investigación es necesario actualizar el estado del arte y seguir unos mínimos de conocimiento disciplinar, temático y metodológico, lo que redunda en buenas investigaciones.

Seguiré, entonces, a Delgado et al. (2005) cuya obra invita a verificar los siguientes interrogantes básicos al realizar un estado del arte:

> 1) ¿Qué campos de indagación se han definido y reconocido como directamente relacionados con el tema de la investigación?, 2) ¿qué conceptos se evidencian como esenciales en los documentos seleccionados para construir el estado de arte? y 3) ¿qué contenidos, tópicos o dimensiones se han definido como prioritarios? (p. 7)

1.1.1. Campos de indagación reconocidos como directamente relacionados con el tema de la investigación.

1.1.1.1. La investigación penal en la sociedad de la información y su materialización a partir de las TIC.

Gamero Casado (2012), al resaltar el uso de las TIC en el ámbito judicial, señala que estas permiten agilizar los trámites de oficina, realizar la gestión documental con mayor rapidez y establecer relaciones con terceros en plazos brevísimos; igualmente, facilitar las gestiones de los profesionales jurídicos y reducir las necesidades de espacio físico laboral; así como suprimir las barreras territoriales y potenciar la igualdad, eliminando obstáculos geográficos que en muchas ocasiones se tornan en verdaderos impedimentos para el acceso a la justicia.

No se trata simplemente de la mera proyección de la administración y la justicia convencional, en papel, a soportes magnéticos, sino de un proceso de mucho más alcance (Criado Grande, 2010). Como ha recordado Valero Torrijos (2007), ante cualquier búsqueda de modernización tecnológica, el rediseño y simplificación de los procedimientos administrativos y judiciales debería convertirse en una prioridad, de la que se derivan exigencias en pro de la supresión o reducción de la documentación requerida a los ciudadanos, así como disminución de plazos y tiempos de respuesta.

Ortiz Pradillo (2013) ha planteado que la utilización de las TIC no es algo nuevo; por el contrario, es el resultado de un proceso de evolución en la humanidad, y esto ha generado la adopción de nuevas formas de investigación criminal con el ánimo de ser más eficientes y eficaces en la lucha contra la delincuencia.

A lo anterior se suma que las formas de ejecución de los delitos han mutado y esas nuevas modalidades, en su mayoría, tienen como instrumento o como fin el manejo de TIC. Así, se evidencia la necesidad de usar tecnología de vanguardia en la investigación judicial, llegando a la vigilancia electrónica u online, conocida como *internet surveillance* (Bellia, 2004); sobre el particular, Llamas Fernández y Gordillo Luque (2007), señalan:

> [...] de la misma manera que hemos pasado de viajar a caballo o en carruaje a utilizar modernas aeronaves que nos permiten alcanzar la órbita exterior terrestre, la policía ha pasado de utilizar linternas y prismáticos a manejar modernas herramientas informáticas y dispositivos electrónicos, tanto en el campo analítico forense (dactiloscopia, balística, etc.), en donde resulta especialmente destacable el manejo de la Informática Forense así como en el campo operativo, a través de lo que se ha venido a denominar la vigilancia electrónica. (p. 236, 2007)

Ortiz Pradillo (2013) también ha indicado que las investigaciones penales tradicionalmente han tenido como principal objetivo la obtención del mayor número de información sobre la comisión de un hecho determinado, esto es, qué sucedió, quiénes intervinieron, cuándo y dónde se produjo la situación.

Por ello, y en la medida en que nos encontramos ante la era de la información, donde las TIC desempeñan un papel determinante, quienes realizan la investigación criminal han denotado interés en poder acceder a toda esa abundante información digital, que diariamente se maneja, para analizarla y utilizarla dentro de la investigación de toda clase de delitos.

En palabras del mismo autor, surge una capacidad nueva: la de "utilizar cualesquiera medidas tecnológicas de investigación destinadas a obtener esa información en formato digital" (p

7). Así pues, Ortiz Pradillo agrega que la operatividad o transversalidad es uno de los elementos esenciales de la investigación criminal en la sociedad informatizada:

> [...] la principal ventaja del empleo de estas nuevas medidas tecnológicas de investigación reside en su operatividad (transversalidad) para la obtención de evidencias de cualquier clase de delito, sea o no de los denominados "delitos informáticos", pues resultan una eficaz herramienta en la investigación de cualquier tipología delictiva en la que tales dispositivos electrónicos constituyan una valiosa fuente de prueba, debido a sus actuales capacidades de almacenamiento de información y a su empleo para todo tipo de comunicaciones. (2013, p. 8)

Es tan relevante el tema que la delincuencia ha sabido adaptarse rápidamente al ciberespacio y a los avances tecnológicos, como lo refiere el autor en comento, hasta el punto de que es preocupante para los principales organismos internacionales (ONU, Unión Europea, etc.) el auge del uso de las TIC con fines delictivos. De hecho, los ataques y el espionaje informático se han convertido en asuntos de interés prioritario para las distintas agencias de inteligencia y de seguridad de los Estados Unidos, sustituyendo por primera vez al terrorismo internacional en la lista de amenazas del país (Arenilla Sáez, 2003). Por esto, se recomienda la regulación clara en cuanto a las investigaciones cuya naturaleza específica incorporen TIC, así como como la profundización de su uso para las propias investigaciones criminales.

Lo anterior llevó a que, hacia 1997, el grupo G8 tomara la decisión de crear un Subcomité encargado de estudiar delitos informáticos (*hightech crimes*), al interior del cual se han generado importantes informes. De igual modo, la Comisión Europea y la Unión Europea (en adelante: UE)

se involucraron de manera activa en el tema; sus principales propuestas se recogieron, inicialmente, en la "Comunicación hacia una política general de lucha contra la ciberdelincuencia" (Comisión Europea, 2007a) y, posteriormente, en el Plan de Estocolmo (Comisión Europea, 2010), dentro del cual la UE retomó la tarea de impulsar medidas frente a la ciberdelincuencia y se dio lugar a la creación del Centro Europeo de Ciberdelincuencia (en adelante: EC3), en la Oficina Europea de Policía (en adelante: Europol), en La Haya (Holanda), según lo ha referenciado Ortiz Pradillo, 2013.

1.1.1.2. La construcción de contextos en la investigación penal.

Sobre la construcción de contextos en la investigación penal se ha escrito mucho; es importante señalar las diversas posturas nacionales al respecto, muchas de las cuales están condensadas en las actas del seminario internacional "Importancia de la construcción de contextos en las investigaciones judiciales", celebrado en Bogotá el 14 de mayo de 2013. Estas recogen el pensamiento de la doctrina nacional e internacional más relevante.

No podría iniciar de otra manera este apartado sino con las palabras de Vargas Silva (2013), quien señala que para construir contextos dentro de las investigaciones penales es necesaria:

> [...] la puesta en marcha de un sistema de investigación novedoso para las víctimas del conflicto, que debe estar apoyada en las experiencias comparadas y en la realidad propia, que debe contener aspectos esenciales de estructura y contenido, como los siguientes:

- Socialización: diseño de estrategias de socialización de los nuevos objetivos de la política criminal desde la interacción y retroalimentación que expliciten metas, propósitos, procedimientos, responsabilidades, etc.

- Enfoque diferencial: la política criminal debe interpretar las diferentes demandas de justicia de las víctimas, pero no, como un concepto vago, interpretado desde la oferta institucional existente, sino concebido desde las características, necesidades, circunstancias e impactos del conflicto en las víctimas.

- Diseño e implementación de mecanismos e instrumentos específicos de coordinación institucional e interinstitucional: vínculos de colaboración en la consecución de objetivos planeados.

- Diseño e implementación de mecanismos de evaluación y seguimiento: incorporar en la construcción del contexto indicadores de proceso y de resultado con participación de representantes de las víctimas, órganos de control, comunidad internacional, etc., que permita compararlo con el sistema de investigación adelantado hasta hoy.

- Diseño e implementación de instrumentos de corrección oportuna: frente a estancamientos o retrocesos en el cumplimiento de metas y cronogramas que permita darle continuidad al proceso y alcanzar los objetivos trazados.

- Capacitación y transparencia: con el fin de que los funcionarios reivindiquen, con una formación, el papel de las víctimas en el proceso judicial y trabajar por restaurar su dignidad.

- Eficiencia: fin primordial de la priorización de situaciones y casos que se refleje en el goce efectivo de las víctimas y no se quede en una evaluación cuantitativa de procesos tramitados.
- Fuentes de información a utilizar y su articulación: ajuste de los sistemas de información a las necesidades planteadas, con acceso ágil, pero seguro, confiable, frente a elementos de orden geográfico, político, económico, histórico, útiles para establecer el contexto.
- Participación de las víctimas: traducida en medidas efectivas en el suministro de información sin temor, ni represalias. (Vargas Silva, 2013, pp. 29-30)

Es oportuno, entonces, resaltar que para el anterior ponente la utilización y articulación de las fuentes de información serán pilares para la construcción de contextos.

Martínez Osorio (2013) establece: "El contexto de cómo sucedieron los hechos consiste en describir la comisión de un acto criminal concreto. Cuanto más clara sea la descripción, más fácil será para el tribunal determinar la responsabilidad" (p. 32); así mismo, señala cuatro aspectos que se requieren: "contextos locales —contexto sociohistórico de los hechos— prácticas y estructura de las organizaciones militares y gestión documental" (p. 33).

Hinestrosa Vélez (2013) dice, en términos generales, que el contexto ha sido utilizado como una metodología o salida, entre jurídica y política, que se prevé en el marco del fin de un conflicto, como en el caso colombiano, el ruandés o el camboyano; o como una salida de un régimen dictatorial a un régimen democrático, como en el caso chileno o de otros países del Cono Sur cuando hicieron su tránsito al régimen democrático.

Por su parte, Wills (2013) se pregunta qué tenemos que reconstruir cuando hablamos de contextos, a lo cual responde que se deben reconstruir las interacciones entre actores, las relaciones fluidas que conectan redes locales a redes nacionales, las estrategias de patrones con bases de datos cuantitativos y los marcos interpretativos que utilizaban los actores para cometer los crímenes, como en el caso de discursos que enmarcan y dan sentido a la acción.

Reed (2013), de la Oficina de la Alta Comisionada de Naciones Unidas para los Derechos Humanos (en adelante: OACDH), refiere que es necesario preguntarse para qué hacer análisis y contextos, y en ese orden explica:

> [...] se trata de utilizar la base técnica de múltiples disciplinas para establecer los elementos relevantes, también de la escena del crimen y creo que no hay que olvidar que debe ser analizada de manera distinta. El estudio de elementos de contexto que tengan un valor explicativo en la ejecución del crimen, su justificación y encubrimiento, la relación o vinculación con otros hechos criminales que puedan ofrecer explicaciones sobre el hecho particular que se está observando o el aparato criminal que fue utilizado para perpetrar un hecho específico, es de suma importancia [...], claramente se busca trascender la escena del crimen. (p. 58)

El mismo Reed (2013) habla de lo que implica organizar bien la distribución de los casos; expresa que los contextos son supremamente útiles como herramienta de coordinación que maximiza los esfuerzos del ente investigador, y contribuyen a la eficiencia procesal.

Así mismo, este doctrinante manifiesta que el segundo momento relevante, luego de la organización, es la estructuración del caso, donde justamente la construcción de los contextos

permite hacer una formulación más amplia e informada de una hipótesis, y desarrollar líneas de investigación estratégicas, no aparentes a primera vista, si eventualmente solo se tuvieran los elementos que rodean al crimen específicamente.

Reed añade que el contexto debe estar determinado por la necesidad de probar; por esto, es importante la interacción con otros procesos, así como dilucidar la existencia de elementos comunes con otros casos y determinar la existencia de patrones con el fin de, ahora sí, plantear conexidades o acumulaciones procesales en las causas, establecer elementos probatorios —que permitan afirmar la existencia de una comunidad de prueba entre las distintas causas analizadas— o simplemente para tener más elementos orientadores del caso específico.

Rameli (2013) señala que la construcción de contextos en la investigación criminal es un elemento angular que impone retos del siguiente tipo: i) Objetividad en el manejo de las diversas fuentes de información[5] 2) Se asume un reto frente a la pregunta ¿qué hacemos con tantos sistemas penales que se tienen en el país? (Ley 600, Ley 906, Ley de Justicia y Paz, Marco Jurídico para la Paz), ¿cómo se hace con tantos sistemas judiciales para la construcción de contextos?[6], y 3) ¿Cómo articular el trabajo de la FGN con la Judicatura?

Aquí corresponde indicar que la FGN emitió la Directiva 02 de 2015, cuyo enfoque es la persecución efectiva de los máximos responsables de la comisión de crímenes de sistema, perpetrados por aparatos organizados de poder, a efectos de conocer la verdad de lo sucedido,

---

[5] "Cuando se construye un contexto se reconstruye la historia colombiana y, en este proceso, puede existir una alta dosis de subjetividad. De allí, la importancia de cruzar diversas opiniones y fuentes de información para eliminar este riesgo y, procurar, al máximo, la objetividad, la cual se logra mediante la planificación, exploración e investigación de diferentes fuentes" (Rameli, 2013, p.81).

[6] Según este siempre habrá manifestaciones que en un marco legal se puede construir, que en el otro no. La idea es que se construya un contexto, independiente de los diversos sistemas procesales, que sea robusto y consistente para los diferentes sistemas normativos.

evitar su repetición y propender por la reparación, así como la investigación y desmantelamiento de organizaciones delictivas responsables de la comisión de múltiples delitos ordinarios; combatir patrones culturales discriminatorios y graves vulneraciones de los derechos fundamentales; enfocar de manera transparente, racional y controlada la acción investigativa de la Fiscalía hacia la consecución de los objetivos anteriormente señalados y, a partir de una política de priorización de casos y situaciones, administrar justicia con eficacia y transparencia hacia la ciudadanía, aplicando herramientas analíticas de gestión y de investigación que permitan el uso adecuado y eficiente de los recursos humanos, administrativos, económicos y logísticos (FGN, 2015).

La Directiva establece, como fines de esta política, modernizar y fortalecer el análisis y la especialización de la investigación penal y del ejercicio de la acción de extinción del derecho de dominio, de tal manera que se incremente la capacidad de la Fiscalía para discernir el impacto de los fenómenos criminales y su judicialización, así como la dificultad de investigarlos y procesarlos con éxito; esta política también contempla adelantar investigaciones integrales con enfoque diferencial de género, étnico, etario, racial, de diversidad sexual y situación de discapacidad, entre otras; de tal manera que se haga efectivo el derecho a la igualdad, tomando en cuenta las características diferenciadoras entre las víctimas y reconociendo que el impacto de las conductas delictivas, al igual que su investigación y judicialización, tienen efectos diversos entre las víctimas de acuerdo con sus contextos socioculturales.

Igualmente, esta Directiva busca adelantar investigaciones con enfoque territorial, que tengan en cuenta las condiciones particulares de las situaciones y casos focalizados, enfatizando en el impacto que la judicialización tendría en las comunidades locales; además, focalizar el trabajo de la FGN en la investigación y judicialización de estructuras criminales, a través de estrategias de investigación analítica en contexto, que permitan caracterizar las estructuras, judicializar a los

individuos responsables que cumplan funciones importantes y extinguir el derecho de dominio de sus bienes, para su desmantelamiento definitivo.

La Directiva en comento también pretende contribuir a la garantía de la seguridad ciudadana a través de investigaciones estratégicas, enfocadas en la identificación de patrones y prácticas criminales, que permitan la judicialización efectiva de las organizaciones criminales que más afectan a la ciudadanía y la extinción del derecho de dominio de sus bienes; coadyuvar en la garantía de los derechos a la verdad, la justicia y la reparación de las víctimas en el marco de procesos de justicia transicional a través de investigaciones judiciales integrales que partan del análisis de los diferentes contextos del conflicto armado (FNG, 2015).

Precisamente, a partir de los presupuestos anteriores se debe señalar que, efectivamente, existe un conjunto de instrumentos que devienen de las normas constitucionales, legales y reglamentarias que desarrollan el ejercicio de la acción penal, las cuales dan vida a la construcción de contextos para integrarlos a las investigaciones criminales.

No obstante, a fecha de hoy, dicha labor se desarrolla de una manera casi rudimentaria y sectorizada, por lo que se hace necesaria la aplicación de la tecnología de procesamiento de información a gran escala que se conoce como *big data*, que nos sirva para la gestión y el análisis de las investigaciones criminales y, de manera específica, para la construcción de contextos, lo que a su vez nos llevará al ejercicio pleno del derecho que tienen las víctimas a la verdad.

1.1.1.3. Big data y análisis de información.

Las diferentes publicaciones sobre de este tema coinciden en indicar términos comunes acerca de la noción de *big data*. Se encuentra, como se ampliará más adelante a través de diferentes autores, que este adelanto involucra el empleo de tecnologías e informática encaminadas a procesar grandes volúmenes de información digital, producida por seres humanos y máquinas, a un bajo costo con respecto al beneficio que presta, con el fin de general análisis y tomar decisiones acertadas al interior de una organización tanto pública como privada.

De la gran variedad de conceptos y explicaciones en torno a este tema, he seleccionado algunos representativos que van desde los más detallados hasta los más simples, todo esto encaminado a llegar al entendimiento de su acepción. Veamos.

Barranco Fragoso (2012) al preguntarse sobre la definición e importancia adquirida en los últimos tiempos del tema en estudio, explica en términos generales que "el concepto de *big data* aplica para toda aquella información que no puede ser procesada o analizada utilizando procesos o herramientas tradicionales" (párr. 1).

Hasta aquí se presenta un concepto muy somero, pero el mismo autor ahonda en que no solo se trata de tener en cuenta que esta implementación tecnológica permite el manejo de un gran volumen de información, sino que también tiene en cuenta la *variedad* de datos, su *velocidad* de procesamiento y la *fuente* de la que estos provienen:

> [...] existe en una gran variedad de datos que pueden ser representados de diversas maneras en todo el mundo, por ejemplo de dispositivos móviles, audio, video, sistemas GPS, incontables sensores digitales en equipos industriales [...] los cuales pueden medir y comunicar el posicionamiento, movimiento, vibración, temperatura, humedad y hasta los cambios químicos que sufre el aire, de tal forma que las aplicaciones que analizan estos

> datos requieren que la velocidad de respuesta sea lo demasiado rápida para lograr obtener la información correcta en el momento preciso. Estas son las características principales de una oportunidad para Big Data. (Barranco Fragoso, 2012, párr. 3)

Camargo Vega, Camargo Ortega y Aguilar (2015), en su texto *Conociendo Big Data*, citan el reporte de Dans (2011), quien define *big data* como "[...] tratamiento y análisis de enormes repositorios de datos, tan desproporcionadamente grandes que resulta imposible tratarlos con las herramientas de bases de datos y analíticas convencionales" (párr. 17).

Así mismo, los mencionados autores relacionan a Zdnet.com para definir *big data* así: "[…] se refiere a las herramientas, los procesos y procedimientos que permitan a una organización crear, manipular y gestionar conjuntos de datos muy grandes y las instalaciones de almacenamiento" (párr. 20). En el artículo en referencia, McKinsey (2012) dice que es necesario prepararse para contratar o reciclar personal, pues las empresas u organizaciones carecen de personas capacitadas en *big data*.

Además, McKinsey (2012), citado por Camargo et al. (2015), "proyecta que para el 2018, solo en Estados Unidos, se necesitarán entre 140 mil y 190 mil nuevos expertos en métodos estadísticos y tecnologías de análisis de datos, incluyendo el ampliamente publicitado papel de científico de datos" (párr. 25). Por su parte, Webster (2012) señala que "[...] las analíticas del *big data* son una nueva forma de hacer inteligencia de negocios[7]" (párr. 12). Así mismo, en el estudio de *Worldwide Big Data Technology and Services* 2013-2017 se proyectaba lo siguiente:

---

[7] Traducción del autor del texto en inglés.

> La tecnología y servicios de Big Data ascenderá con una tasa anual de crecimiento compuesto del 27 % hasta llegar a los 32.400 millones de dólares en 2017, unas seis veces la tasa del mercado general de tecnologías de la información y comunicaciones (computerworld.es, 2013).

De otro lado, en una columna escrita por Gallardo (2013) se indican los pasos para la implementación de *big data*:

1. Entender el negocio y los datos. Este primer paso pide un análisis detallado con las personas que hoy laboran y entienden los procesos y los datos que la empresa maneja.
2. Determinar los problemas y cómo los datos pueden ayudar.
3. Establecer expectativas razonables, es decir, definir metas alcanzables; esto se puede lograr si al implementar la solución de un problema, este no presenta alguna mejora, y se debe buscar otra solución.
4. Cuando se inicia un proyecto de *big data* es necesario trabajar en paralelo con el sistema que hoy está funcionando.
5. Al tratar de implementar un proyecto de *big data* se debe ser flexible con la metodología y las herramientas; esto se debe a que las dos anteriores son recientes y pueden llegar a presentar problemas al implementarlas.
6. Es importante mantener el objetivo de *big data* en mente; esto porque el proceso es pesado y porque (sic) no es tedioso, máxime cuando los métodos y herramientas

que usan *big data* para el análisis de datos aún pueden presentar problemas, y la idea es que se mantenga en mente la meta final del proyecto sin desanimarse pronto.

Por su parte, el centro de investigaciones Gartner (2012) define *big data* como "un gran volumen, velocidad o variedad de información que demanda formas costeables e innovadoras de procesamiento de información que permitan ideas extendidas, toma de decisiones y automatización del proceso".

Según Forrester (2013), citado por el informe de Gartner (2013), el *big data* incluye las técnicas y tecnologías que permiten que sea económico manejar datos a una escala extrema. Según este autor dicha solución informática consiste esencialmente en:

> [...] i) Las técnicas, la tecnología y personal calificado que lo hace posible; ii) Escala extrema de datos que supera a la tecnología actual debido a su volumen, velocidad y variedad; iii) El valor económico, haciendo que las soluciones sean posibles.

El *big data* es, pues, aquel tratamiento masivo de datos, para un fin determinado, utilizando herramientas tecnológicas avanzadas, personal idóneo y calificado, con un presupuesto bajo en relación con el beneficio, ya que se genera bajo parámetros de velocidad, variedad, volumen y veracidad.

Lo anterior es confirmado por TRC Informática (s.f), cuando refiere que el vicepresidente de la consultora IDC, Phillip Carter, expresa que big data es "una nueva generación de tecnologías y arquitecturas diseñadas para extraer valor económico de grandes volúmenes de datos heterogéneos habilitando una captura, identificación y/o análisis a alta velocidad" (p. 2).

Finalmente, Salgado, en entrevista con Gómez (2014) para la revista Computerworld, explica sencillamente que este conjunto de tecnologías "consiste en consolidar toda la información de una organización y ponerla al servicio del negocio" (párr. 4).

En cuanto a la implementación del big data en entidades del Estado, según la Oficina contra la Droga y el Delito de Naciones Unidas (2010), en los últimos 50 años se ha ido refinando sistemáticamente el uso de la información y la inteligencia policiales. Los sistemas de información policial, que antes se basaban en el cotejo de fichas a cargo de un archivero, han evolucionado con las TIC hasta convertirse en departamentos que utilizan programas informáticos especiales y las competencias de analistas profesionales del delito.

También se ha evolucionado en la aplicación de la información; se han desarrollado técnicas y metodologías de inteligencia para detectar amenazas delictivas y trazar el perfil de delitos y delincuentes conocidos. Desde el punto de vista estratégico y táctico, actualmente se dispone de inteligencia que le permite a la Policía adoptar decisiones más exactas y más fáciles de justificar.

Un ejemplo de lo anterior es lo que ha sucedido en Colombia, donde la Policía Nacional, con más de 180.000 servidores, se enfrentaba al reto de correlacionar toda la información procedente de diferentes fuentes: desde cámaras de video vigilancia hasta llamadas a la Línea de Atención 123 y flujos de trabajo del personal en las calles.

Para dar respuesta a este requerimiento, la Policía diseñó un proyecto de *big data* para transformar esa información en conocimiento. Así lo explicó, en su momento, el director de TI de la Policía Nacional, Jairo Gordillo (Villarrubia, Datacenter Dynamics, 2014).

1.1.1.3.1. Dimensiones del big data.

En relación a las dimensiones o componentes del *big data*, como elementos esenciales y transversales a una gran cantidad de información, tal como se mencionó, se encuentran el volumen, la variedad, la velocidad y la veracidad de los datos. El primero de ellos hace referencia a las cantidades masivas de datos que las organizaciones intentan aprovechar para mejorar la toma de decisiones en toda empresa, tanto privada como pública (Romero-Morales, Smart, Shockley, Schroeck, y Tufano, 2012)

De manera práctica, se puede afirmar que el volumen alude al tamaño de la información (TRC Informática, s.f.). La variedad tiene que ver con gestionar la complejidad de múltiples tipos de datos, incluyendo los semiestructurados y no estructurados (Recuperación de Información en Internet, 2011); se trata de diferentes datos en innumerables formas, como texto, datos web, tuits, datos de sensores, audio, video, secuencias de clic, archivos de registro y mucho más (Romero-Morales et al., 2012).

La velocidad en la creación y análisis del *big data* es el dinamismo que permite disponer la información en tiempo real y generar estudios bastante detallados y complejos, que a menudo se integran en los procesos de trabajo y los sistemas.

Los datos se generan de forma continuada, un ejemplo de ello podría ser cuando damos un "me gusta" en una red social, allí se están creando nuevos datos; de igual modo sucede cuando se emplea el GPS o con la compra de un tiquete de avión, etc. Cada uno de estos eventos producen datos de forma constante y real (Ortoll, 2014).

Por último, la veracidad hace referencia al nivel de fiabilidad asociado a cierto tipo de datos, la calidad de estos es un requisito importante y un reto fundamental del *big data* (Romero-Morales et al., 2012).

1.1.1.3.2. Elementos.

Así como existen componentes o dimensiones del *big data*, hay elementos que facilitan el análisis de la información (Protocolos y capas, 2017); los más reconocidos son: (i) La fuente, reconocida como el origen de los datos, que pueden provenir de registros históricos, almacenes de datos, dispositivos inteligentes, sistemas de gestión de datos e internet; (ii) capa de almacenamiento, cuya función es la de recoger y transformar los datos sin perder de vista la normativa legal; (iii) capa de análisis, se encarga de leer los datos almacenados; mediante la utilización de los modelos, los algoritmos y las herramientas adecuadas, proporciona visibilidad sobre los datos para que puedan ser consultados en la capa de consumo.

Y está el elemento final: (iiii) la capa de consumo, es decir, la utilización de los datos, donde los proyectos y usuarios se benefician del conocimiento extraído en todo este proceso. La forma de consumir los datos dependerá del destinatario, pero será habitual verlos en forma de *reporting* o visualización en tiempo real (Mora, 2016).

1.1.1.3.3. Fases

Los diferentes tipos de análisis siguen un conjunto de fases comunes que ayuda en la toma de decisiones (Rayo, 2016). Se trata de pasos que deben seguir las empresas o entidades para la organización de la información, estos son: adquisición de datos y grabación, extracción y pre-procesamiento de la información, representación, agregación e integración de datos,

procesamiento de peticiones, análisis de datos y, por último, su interpretación. Esta última fase está directamente relacionada con el *data mining* o minería de datos, donde hay una multitud de tareas; entre estas están las tendientes a manipular, procesar, modelar, analizar y extraer la información que se necesite dado un problema determinado (Fases en big data y librerías hadoop, s.f.).

1.1.1.3.4. Algunas técnicas

Entre las técnicas más comunes para el tratamiento masivo de datos o información encontramos: *Machine Learning y Hadoop Map Reduce*, la primera se conoce como una técnica para conseguir el aprendizaje automático basado en datos (López, 2014); se trata de una disciplina científica del campo de la inteligencia artificial que crea sistemas que aprenden automáticamente. En este contexto, *Aprender* quiere decir identificar patrones complejos en millones de datos; **la máquina que realmente aprende es un algoritmo** que revisa los datos y es capaz de predecir comportamientos futuros. *Automáticamente*, también en este contexto, implica que estos sistemas se mejoran de forma autónoma con el tiempo, sin intervención humana (González, 2014).

Por su parte *Hadoop* es un sistema basado en el procesamiento paralelo de grandes conjuntos de datos (Camargo Vega et al., 2015). Es un sistema de código abierto que se utiliza para almacenar, procesar y analizar grandes volúmenes de datos; sus componentes básicos son: (i)HDFS: consiste en un sistema de archivo distribuido, que permite que el fichero de datos no se guarde en una única máquina, sino que sea capaz de distribuir la información a distintos dispositivos. (ii) Mapreduce: se trata de un marco de software de trabajo que hace posible aislar al programador de todas las tareas propias de la programación en paralelo, es decir, permite que un programa, que ha sido escrito en los lenguajes de programación más comunes, se pueda ejecutar

en un conjunto de *Hadoop*. Este sistema tiene la gran ventaja de permitir escoger y utilizar el lenguaje y las herramientas más adecuadas para la tarea concreta que se va a realizar en *big data*.

De acuerdo con la información presentada, una solución de *big data* se presenta como idónea ante los retos de la Fiscalía General de la Nación, que incluyen el análisis de contextos alimentados por un gran flujo de información dentro de la investigación criminal; por ello, se hace urgente que el marco jurídico sea más específico para propiciar la inclusión de este conjunto de tecnologías, que además soporten un sistema de ciberseguridad.

2. Contenidos marco y dimensiones prioritarias actuales en la Fiscalía General de la Nación

2.1. Estado actual de la estrategia de investigación criminal en relación con el objetivo estratégico de la FGN

Para entender la estrategia de la FGN debe partirse de la función constitucional del ejercicio de la acción penal y su participación en el diseño de la política criminal del Estado, esta se ve reflejada en la Resolución 738 de 2017, por la cual se aprobó el direccionamiento estratégico de la entidad para la vigencia 2016-2020, denominado La Fiscalía de la Gente, por la Gente y para la Gente[8], según lo estipula su artículo 1° (FGN, 2017).

De acuerdo con dicho acto administrativo, que fija el rumbo del ente investigador, la misión y la visión cambiaron con respecto al periodo anterior y están alineadas con la nueva planeación, vigente para el cuatrienio señalado, así como incluidas en esta.

Así las cosas, la misión publicada actualmente en el sitio web de la entidad, y por ende vigente, es del siguiente tenor:

> La Fiscalía General de la Nación ejerce la acción penal y de extinción de dominio en el marco del derecho constitucional al debido proceso; participa en el diseño y la ejecución

[8] El numeral 8 señala que el Plan Estratégico tiene cinco partes:
[...] en la primera de ellas se presenta un diagnóstico resumido de los principales focos de criminalidad que debe enfrentar la FGN en los siguientes años y plantea algunos principios transversales que orientarán el accionar institucional. La segunda parte describe la metodología utilizada para desarrollar la planeación estratégica concretada en este Plan. La tercera parte sintetiza la misión, visión y los valores de la institución. La cuarta y quinta parte describen los objetivos estratégicos y de gestión que la entidad logrará en los siguientes cuatro años [...] (FGN, 2016b, p. 6)

de la política criminal del Estado; garantiza el acceso efectivo a la justicia, la verdad y la reparación de las víctimas de los delitos; y genera confianza en la ciudadanía. (FGN, s.f.)

Debo resaltar algunos de los aspectos del Plan Estratégico de la FGN que tocan trasversalmente el desarrollo de la presente investigación; por ejemplo, el numeral 19 establece como principio la "reingeniería institucional y aumento de la productividad", sobre este expone:

> Un mejor manejo de la carga de trabajo implica aumentar la productividad de la entidad y hacer un seguimiento riguroso a las tareas de investigadores y fiscales. Aumentar la productividad y la eficiencia supone una reingeniería institucional profunda que permita que la definición de tareas y metas individuales sumadas a un efectivo trabajo en equipo contribuyan a los objetivos estratégicos de la entidad. Para lograr un aumento en la productividad se deben optimizar procesos, eliminando pasos innecesarios y **contar con los recursos tecnológicos** óptimos **para aplicar criterios de priorización y desarrollar investigaciones más analíticas**. Todo esto acompañado de mecanismos de control ágiles y que faciliten la comunicación [...] (FGN, 2016b, p. 16) *(Negrillas ausentes del texto original.)*

Así mismo, el numeral o párrafo 20 de dicho Plan establece "la austeridad estratégica" como otro principio, acerca del cual cabe destacar:

> [...] el manejo estratégico de la carga de trabajo no sólo debe contribuir a mejorar el desempeño de la FGN en delitos más graves y más complejos, sino que esta aproximación a la investigación y ejercicio de la acción penal y de extinción de dominio debe traducirse

> en la asignación más eficiente de los recursos disponibles. En este sentido, la inversión se concentrará en aumentar la capacidad tecnológica de la entidad [...] (FGN, 2016b, p. 17)

Igualmente, El Plan Estratégico, en su párrafo 22, señala que las prioridades en investigación y judicialización están relacionadas con los siguientes puntos:

> Impactar de forma contundente el crimen organizado; impactar la corrupción; combatir la violencia como un fenómeno priorizado de la seguridad ciudadana; y contribuir a la terminación del conflicto armado sin impunidad. (2016b, p. 17)

Así, surge la necesidad de contribuir al cumplimiento de la actual visión institucional (2017-2020) —plasmada en el párrafo 29 del mencionado Plan Estratégico y publicada también en su sitio web— la cual expresa que la entidad:

> [...] será reconocida por su modelo de gerencia pública, su transparencia y su apoyo decidido a la paz. Habrá reducido significativamente la impunidad, mediante el combate y desmantelamiento de las organizaciones criminales, la lucha contra la corrupción y sus aportes a la seguridad ciudadana, **apoyada en tecnologías de punta** y un talento humano al servicio de la gente. (FGN, 2016b, p. 7) *(Subrayado y negrillas ausentes del texto original.)*

Del mismo modo, se deben resaltar los Objetivos estratégicos, que de acuerdo con el párrafo 21 del documento se refieren a:

> [...] cuatro prioridades en investigación y judicialización; tres objetivos para mejorar la gestión misional de la entidad y fortalecer la presencia territorial de la FGN y cuatro

objetivos para mejorar la gestión administrativa de manera tal que se logren administrar los recursos con austeridad estratégica. (FGN, 2016b, p. 17)

Por lo anterior, es conveniente presentar el listado de los Objetivos estratégicos que se encuentran explicados a lo largo del Plan en comento:

Objetivos estratégicos:

1. Impactar de forma contundente el crimen organizado.
2. Impactar la corrupción de mayor impacto.
3. Combatir la violencia como fenómeno priorizado.
4. Contribuir al fin del conflicto armado sin impunidad.
5. Mejorar el acceso a la justicia.
6. Fortalecer la acción penal en el territorio.
7. Consolidar políticas de manejo estratégico de la carga de trabajo.
8. Gestionar y optimizar los recursos financieros.
9. Fortalecer la infraestructura tecnológica.
10. Optimizar los procesos y fortalecer el Sistema de Gestión Integral.
11. Desarrollar el talento humano. (FGN, 2016b)

Son precisamente estos objetivos los que dan vida y fundamento al desarrollo de proyectos de investigación como el presente, para cuyo propósito el noveno se destaca especialmente, puesto que se denomina "Fortalecer la infraestructura tecnológica".

Entre los elementos estructurales de dicho objetivo, refiero el contenido en el párrafo 124, referente a la descripción del mismo y que explica que su finalidad consiste en "[...] lograr que la

FGN cuente con un sistema de información unificado que garantice la integridad, disponibilidad, confidencialidad y oportunidad de la información a nivel nacional [...]" (FGN, 2016b, p. 46).

En consecuencia, este objetivo también pone de presente la necesidad definir y diseñar la arquitectura institucional de la entidad, por lo que el párrafo 127 expresa que se debe:

> [...] realizar un diagnóstico y formular un plan tecnológico a mediano plazo que le permita: i) gestionar adecuadamente los procesos penales, ii) aplicar herramientas vigorosas de análisis criminal y ii) tomar decisiones gerenciales y estratégicas con base en evidencia empírica sólida [...] (FGN, 2016b, p. 46)

Según lo visto, la FGN a la fecha cuenta con instrucciones y sistemas que, si bien tienen como finalidad el cumplimiento de los objetivos estratégicos, resultan mínimos frente a los compromisos que se adquieren con la nueva estrategia investigativa y los nuevos retos que demanda un país en paz.

2.1.1. Uso de TIC en la Fiscalía para actividades de recolección, gestión y análisis de información con el fin de construir contextos.

Como se ha referido, el actuar de las autoridades públicas, para nuestro caso de la FGN, se debe fundamentar en la legalidad; por esto, es importante iniciar este apartado recordando que la Resolución 1343 de 2014 establece unas actividades tendientes a determinar si una situación o un caso investigativo debe ser priorizados o no, estas son:

> i) Fijar un orden en el que serán atendidos; ii) destinar un alto número de funcionarios o mayores herramientas de trabajo; iii) destinar mayores recursos para agrupar e investigar de manera conjunta casos asociados; iv) aplicar herramientas analíticas en el trámite,

investigación y judicialización; v) enfocar los esfuerzos de investigación y judicialización en ciertos casos o hechos delictivos y vi) enfocar los esfuerzos de investigación o judicialización en algunos de los presuntos responsables (FGN, Resol. 1343, 2014).

Si se observa, se proponen los elementos de análisis en contextos y herramientas analíticas en el marco de las investigaciones que se adelantan; tales elementos se han desarrollado como instrumentos para fiscales, investigadores y asistentes de fiscal, pero no están integrados a la labor investigativa llevada a cabo por la Policía Judicial, que muchas veces es realizada manualmente y sin previsión de que los resultados pueden llegarse a utilizar como prueba e incluso ser objeto de pérdida o hurto, y terminar en las manos de terceros interesados en los mismos, por ejemplo, organizaciones criminales que quieran los datos de análisis de las investigaciones para cambiar su modo de operar.

Se plantea al interior de la FGN que estas herramientas parten de aplicar tres elementos metodológicos tendientes a la construcción de contextos. El primer elemento consiste en ampliar el foco de la investigación a partir de entender que los hechos delictivos no ocurren de manera aislada, sino que se explican a partir de su contexto y, de acuerdo con esto, hay que plantear hipótesis de trabajo para confirmarlas o rechazarlas a través del análisis de la información y evidencia disponibles.

Otro elemento metodológico indica que se requiere disponer de diversas fuentes de información y ser riguroso con su uso: analizar elementos materiales probatorios (en adelante: EMP), evidencia física (en adelante: EF) e información proveniente de fuentes formales y no formales que den cuenta de los hechos delictivos y su contexto; finalmente, se deben emplear otras disciplinas para explicar fenómenos criminales, situaciones y casos, lo que incluye la

aproximación de las ciencias sociales y exactas para comprender el delito e ilustrar la teoría del caso (FGN, Resol. 1343, 2014).

Las herramientas existentes desarrollan las técnicas para identificación de fenómenos criminales, delimitación de situaciones y asociación de casos; aquellas también permiten la caracterización de situaciones a partir de patrones, así como la de víctimas y estructuras criminales. Realizaré una aproximación a cada una de ellas.

2.2. Herramientas en cuanto al análisis

2.2.1. Cómo identificar fenómenos criminales y estudiar los resultados desde las tecnologías de la información.

Hasta ahora se ha planteado al interior de la Fiscalía General de la Nación que este apartado se funda en el análisis criminal estratégico para identificar problemáticas a mediano y corto plazo así como sus tendencias; se trata de un elemento clave para que los comités de priorización puedan tomar decisiones estratégicas basadas en fenómenos; no solo en delitos, sino en la relación entre estos, tendiendo a buscar un análisis integral y no caso a caso; por lo cual, se establece que se deben agotar cuatro pasos:

1. Determinación de resultados de la FGN por tipo penal.
2. Determinación de fenómenos criminales (incluye actividades con consecuencia delictual, factores geográficos, económicos, sociales, culturales y tecnológicos que

facilitan la comisión de las conductas criminales, el conjunto social afectado y los posibles autores).

3. Análisis de oportunidad o dificultad para investigar el fenómeno.
4. Aplicación de test de priorización, a partir de los elementos subjetivos, objetivos y complementarios.

Entonces, ¿cómo realizar dicho procedimiento a partir de la utilización de tecnologías cuando los sistemas existentes no son interoperables?

2.2.2. Delimitación de situación y asociación de casos.

A pesar de que no se cumplan los requisitos para que se decreten figuras procesales como la conexidad, o cuando por el tipo de procedimiento sea menester tramitar noticias criminales de manera independiente, a partir de la relación analítica de casos asociados entre sí, y teniendo en cuenta las circunstancias de tiempo, modo y lugar en que suceden los hechos, se desprende la posibilidad de cambiar el foco de investigación y pasar de un examen individualizado a la delimitación de una situación, y por qué no, a una relación entre unos hechos y otros (FGN, Unidad Nacional de Análisis y Contextos, 2013).

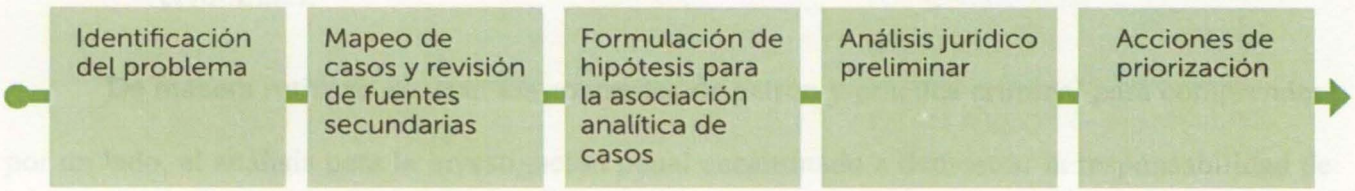


Figura 1: De cartilla 5. Herramientas analíticas para la investigación y ejercicio de la acción penal (FGN, 2015a)

La identificación del problema está vinculada a la determinación del hecho jurídicamente relevante para el derecho penal, es decir, aquel hecho que reviste la característica de delito y que se encuentra tipificado en el ordenamiento jurídico.

El mapeo se centra en la búsqueda, en los sistemas misionales de información, que puede tener relación con los hechos materia de investigación inicial; a partir de ello se formula una hipótesis delictiva, lo que conlleva la posibilidad de delimitar una situación a partir de la cual se puedan asociar los casos; una vez sucede esto, se procede a la evaluación de situaciones jurídicas procesales para determinar de qué forma se pueden trabajar los distintos asuntos en conjunto.

Por último, se encuentra la evaluación de los elementos subjetivos, objetivos y complementarios que pueden llevar a la variación de asignación de ciertas investigaciones en un solo despacho, la conformación de un grupo de tareas especiales que pueda adelantar las investigaciones de forma asociada o la focalización de la investigación en ciertos hechos delictivos por parte de un fiscal. Así, la configuración de una situación puede servir para el trabajo conjunto entre varios despachos encargados de la investigación sobre distintos elementos de una misma hipótesis criminal.

2.2.3. Determinación de situaciones a partir de la identificación de prácticas y patrones criminales.

De manera rutinaria se usan los conceptos de patrón y práctica criminal para comprender, por un lado, el análisis para la investigación penal encaminado a demostrar la responsabilidad de una conducta punible y, por otro, el análisis del delito para la acción de la Policía, cuyo fin es el

cumplimiento de actividades preventivas, desde la identificación de tendencias o ilustración de nuevos fenómenos.

Esta situación se materializa a través de la identificación de:

a. Practicas criminales cuyo objeto determinante son las coincidencias entre las circunstancias de tipo temporal, modal y espacial, asociadas a un grupo delictivo específico.
b. Patrones criminales, determinados por los móviles y componentes del plan criminal asociado al hecho.

Tabla 1
Diferencias entre la identificación y caracterización de práctica y patrón

Características	Práctica	Patrón
Definición	Conjunto reiterado de hechos delictuales de idéntica o análoga naturaleza que estén conectados entre sí de manera tal que no puedan ser reducidos a incidentes aislados o excepcionales.	Conjunto de semejanzas compartido entre dos o más delitos y que puede identificarse a partir de la articulación analítica entre diferentes variables (agresor, víctima; bienes y *modus operandi* utilizados, entre otros).
Información Requerida	Descripción de la fecha, lugar, frecuencia, modo, tipo de víctima y tipo de agresor de los delitos.	Descripción cuantitativa y cualitativa sobre la forma de ocurrencia de los delitos haciendo énfasis en la forma de operar del agresor, el objetivo perseguido y los criterios de selección de la víctima.

Contribución a la investigación criminal	Orienta la recolección de EMP e información en lugares coincidentes.	Aporta elementos sobre los móviles, el plan criminal y los posibles responsables de un grupo de delitos.

Nota: Reelaborado a partir del Cartilla 5. Herramientas analíticas para la investigación y ejercicio de la acción penal. (FGN, 2015a, p. 22)

2.2.4. Caracterización de víctimas.

El objetivo de esta es diferenciar los efectos del delito sobre la población catalogada dentro de grupos especiales en razón a situaciones de tipo histórico, social, cultural, religioso, político, étnico, que puedan plantear una discriminación; con esto se busca: i) focalizar esfuerzos y recursos; ii) focalizar hechos y servir como elemento para asociar casos y delimitar situaciones. Por ello es fundamental, dentro de las actividades por desplegar, identificar los siguientes elementos:

a) Determinar datos demográficos como género, etnia, edad, filiación, condición social y económica.
b) Trayectoria biográfica de la víctima.
c) Determinación del entorno de vida.
d) Determinación del entorno social, político y económico de la víctima.
e) Determinación del número de víctimas.

2.2.5. Identificación de estructuras criminales.

Debe entenderse que una estructura criminal es un conjunto de personas que actúan de forma concertada para cometer uno o más delitos, de manera permanente, delimitada jerárquica,

rígida o flexiblemente, con códigos de conducta y un sistema de toma de decisiones que asegura el cumplimiento de las órdenes.

Para la identificación de las estructuras —siguiendo la Cartilla n° 5 de herramientas analíticas para la investigación y ejercicio de la acción penal, de la FGN— se deben seguir los siguientes pasos:

> (i) Identificar y definir los atributos que caracterizan a las estructuras criminales, (ii) compartir y complementar estas definiciones con otras entidades y expertos en criminalidad organizada, (iii) ordenar los atributos por orden de afectación a los derechos a las víctimas o a la seguridad ciudadana, (iv) dar valores cualitativos (Alto, Medio, Bajo, Inexistente, Información Insuficiente) para cada uno de los atributos, (v) caracterizar cada una de las estructuras criminales identificadas de acuerdo con los atributos y los valores acordados, y (vi) introducir los resultados de la caracterización en una matriz de fácil observación para los tomadores de decisión. (FGN, 2015a, p.34)

Frente a lo anterior, es importante delimitar los fines que persigue la estructura criminal, así como sus dinámicas regionales, logística, comunicaciones, apoyos, e interacción, y su relación con otras estructuras.

2.3. Los sistemas de información misional como instrumento para la gestión, recolección y análisis existentes en la FGN y su desconexión con la estrategia de e-justicia.

2.3.1. EL SPOA.

Es el sistema de información que registra las actividades de investigación seguidas por el procedimiento general de investigación de la Ley 906 de 2004; este no se cruza con las informaciones registradas en los sistemas de información de Ley 600 de 200 ni de la Ley 975 de 2005.

De acuerdo con el Manual de usuario de este sistema, su objetivo es facilitar la forma de ejecutar las tareas relacionadas con el Sistema Penal Acusatorio, en cuanto al registro de la actividad de investigación de los diferentes organismos de Policía Judicial y el Instituto de Medicina Legal; así como con datos de registro de elementos probatorios, actuaciones o actos de investigación y control de términos de la FGN, al igual que las decisiones e información referente a las etapas de juzgamiento y ejecución de penas (FGN, 2013).

Lo anterior quiere decir que su concepto inicial fue servir de soporte administrativo para la ejecución de las actividades investigativas, pero en absoluto se ha constituido como un instrumento incorporado al actuar estratégico en las investigaciones penales.

En los anexos A se puede observar, en cada uno de los módulos, el elemento numérico o de registro administrativo, pero no se evidencia la posibilidad de realizar un análisis de la información allí consignada.

Igualmente, en el SPOA están los módulos de reparto y de almacén. En el primero se registra el reparto de las noticias criminales asignadas a cada despacho fiscal; en el segundo, se incluyen las informaciones relacionadas con los EMP, EF de cada una de las investigaciones sometidas a cadena de custodia.

En cuanto al módulo específico de consultas, estas se permiten por los diferentes criterios, pero no cuenta con la posibilidad de hacer análisis de estos datos, es decir, el sistema muy estático

y nada dinámico en cuanto al análisis de las informaciones para la toma de decisiones estratégicas. (Ver anexos A)

En las tablas 2 y 3 de la sección Tablas y Figuras, de este documento, se pueden ver ejemplos de cómo se ha estructurado el resultado de las informaciones de los sistemas de información con meros efectos estadísticos de producción; así, la Cartilla n. 4 de Construcción y Análisis de Indicadores de Carga de Trabajo (FGN, 2015b) es el fiel reflejo de ello, según se puede observar en las tablas en mención. En los términos señalados en la misma cartilla se presentan cuatro herramientas que orientan la construcción y el análisis de indicadores de carga de trabajo para tomar decisiones de priorización:

> [...] i) Diseño de indicadores, ii) selección y cálculo de indicadores de carga de trabajo, iii) identificación de dificultades en la investigación y judicialización para la toma de decisiones de priorización y iv) uso de indicadores de carga de trabajo para seguimiento y evaluación de la política de priorización. (FGN, 2015b, p. 5)

Estos indicadores permiten, en palabras de la misma cartilla desagregar por delitos, por periodos de tiempo o por dependencias, y tienen un enfoque en tres aspectos particulares: i) el inventario de los procesos que entraron a la FGN, ii) el flujo de dichos procesos a lo largo del procedimiento penal y iii) la distribución entre despachos o unidades del inventario de procesos.

La misma cartilla muestra (a través de las tablas aludidas) cómo los datos de los sistemas de información son cuantitativos en cuanto a la carga administrativa de los despachos, pero nada más que ello.

Pese a que el sistema de información solo realiza un análisis cuantitativo, mas no cualitativo, para dar cumplimiento a las actividades señaladas previamente, sí dispone de un apartado para determinar que la carga de trabajo permite realizar un test de priorización; cuestión que está totalmente desencajada de una estrategia para utilizar tecnologías en la investigación criminal, como se ha dicho, y más aún para realizar analítica que permita la toma de decisiones estratégicas en cuanto a la asociación de casos, determinación de patrones y situaciones.

2.3.2. EL SIJUF.

Es el sistema de información para funcionarios y servidores de la FGN que tiene por objetivo registrar las actuaciones de investigación de los procesos que se siguen en el marco de la Ley 600 de 2000. Este sistema de información cuenta con registros e informaciones que no se cruzan con los sistemas de información SPOA y SIJYP, debo referir de manera muy concisa que este sistema de información cada vez más está en desuso pues los procesos que se siguen por dicho procedimiento, en su regla general, corresponden a hechos acaecidos con anterioridad al año 2005, pero de todas formas representan un porcentaje importante de las investigaciones que se llevan.

Sin embargo, hay poco que decir pues el sistema cuenta con pocas facilidades para su interoperabilidad con los otros.

2.3.3. SIJYP.

Sistema de información para funcionarios y servidores de la FGN que tiene por objetivo registrar todas las actuaciones de investigación de los procesos que se siguen en el marco de la Ley 975/2005 de Justicia y Paz. Este sistema de información cuenta con registros e informaciones que no se cruzan con los sistemas de información SPOA y SIJUF.

Actualmente, la FGN cuenta con un servicio de análisis criminal cuyo objetivo principal es la realización de análisis: de campo, operativo, comparativo de casos, de caso, delictual, telefónico y de personas, así como análisis estratégico; su finalidad principal también abarca consulta de información y servicio de consulta de información en bases de datos privadas con las que la FGN tiene convenios establecidos. Sin embargo, esta no se realiza de manera generalizada dentro del conjunto de investigaciones, esto es, buscando correlaciones entre unas y otras, determinando patrones y elementos comunes, etc.

3. La necesidad de implementar un expediente judicial electrónico que soporte las actividades de recolección, gestión y análisis de la información

Al menos en las sociedades occidentales internet se ha convertido en algo "esencial para la vida", tal como lo afirmó el Tribunal Superior Alemán el 24 de enero de 2013, y los datos no hacen más que confirmar esta tendencia. Los números dan la razón: a finales del 2012, en el mundo, alrededor de 2.500 millones de personas estaban en línea (incremento del 10% anual), 241 millones más que el año anterior (Fundación Telefónica, 2014, p. 34).

El mismo informe publicó que en América había 998 millones de usuarios de telefonía móvil (105%) y 542 de internet (57%), (Europa con 768 millones, 123% y 443 millones, 71%, respectivamente).

Así mismo, datos de junio 2012 (internetworldstats, 2012), señalaban que un 48% de la población de América Latina estaba ya conectada a internet. La media de acceso en Europa, según esos datos era de 63 puntos y de Norte América 78% (68.6% en 2006).

Para 2013 se estimaba que casi el 40% de la población mundial estaría conectada a Internet. El porcentaje de personas que utilizaba internet en los países desarrollados alcanzó a, finales de 2012, el 73, 4%. En términos absolutos, casi la mitad de los conectados a internet en el mundo estaba en Asia Pacífico, siendo 1.133 millones en 2012 (ITU, 2012).

Por países, para 2012, en América Latina el escenario, en cuanto a conexión a internet, era este: Argentina (68%), Colombia (59%), Chile (58%), Uruguay (56%). Estos países se destacaban entre los de mayor penetración de este medio de comunicación (Internetworldstats, 2012), con

16,8 millones —36,6%— de usuarios de *Facebook*. La evolución en diez años ha sido casi geométrica, como puede apreciarse.

A corte 2016 (Fundación Telefónica, 2017), la banda ancha de nueva generación es ya mayoritaria y relaciona las tendencias del mercado; se resalta que la banda ancha de nueva generación (FTTH+HFC), con 6,74 millones de líneas, supera al DSL (6,67 millones de líneas) a corte agosto de 2016; igualmente, la mensajería instantánea se ha empezado a emplear más en el ámbito empresarial.

De acuerdo con dicho informe, uno de cada tres internautas ya se comunica con empresas utilizando aplicaciones de mensajería instantánea, cifra que aumenta a uno de cada dos entre los más jóvenes. Por otra parte, los sistemas inteligentes y robots empiezan a aprender la cultura y valores de nuestra sociedad; un ejemplo de esto es como en la Universidad de Berkeley se estableció un centro de investigación para facilitar que los robots aprendan los valores humanos.

Este documento señala que ya hay dispositivos y sensores que se pueden introducir en cuerpo humano y que ofrecerán capacidades sobrenaturales. De hecho, más de 10.000 personas llevan insertado, debajo de la piel de la mano, un pequeño chip con tecnología NFC o RFID.

Los jóvenes recurren a Internet como herramienta para su formación; durante 2016, se observa un agotamiento en el uso de las redes sociales con una levísima disminución media de su uso del, 0,1%. En los grupos de los más jóvenes, que generalmente marcan tendencia, esta disminución es más importante y es de 2,2 puntos porcentuales entre los internautas entre 14 y 19 años, y de 7,9 entre aquellos entre 20 y 24 años.

Igualmente, el informe de Telefónica resalta que el mundo digital y real se fusionan, el 78% de los internautas utiliza la mensajería instantánea para concertar encuentros o salidas; el

correo físico se convierte en pasado para los más jóvenes, el porcentaje de internautas entre 14 y 19 años que utilizan el correo físico pasa del 10,2% a 2,8%.

De acuerdo con el documento en mención, internet impulsa la vida social, dado que el 55,7% de los internautas afirma que gracias a este medio de comunicación se ha vuelto a relacionar con familiares y amigos de toda la vida. Igualmente, se expresa que el 36,7% de los internautas ha encontrado buenos amigos utilizando la web; el 35% ha encontrado compañeros profesionales; el 32,3%, compañeros para participar en actividades de ocio e incluso, un 9,8%, compañeros para participar en actividades de tipo político, y 28,7% de los jóvenes, entre 20 y 24 años, ha encontrado pareja en internet.

El móvil revoluciona la forma en la que nos organizamos; el 79,5% de usuarios, entre 14 y 19 años, toma decisiones no planificadas, sobre la marcha, relacionadas con el ocio gracias a información que recibe continuamente en el móvil. Este dispositivo rompe las barreras entre la vida profesional y personal; el 79% de aquellos que tienen móvil de empresa, lo utiliza para su vida personal; 94,2%, entre 55 y 64 años. El 68% instala aplicaciones personales en el móvil de empresa, 85,7%, entre los usuarios entre 25 y 34 años. Llega la revolución del marketing de la mano de las nuevas tecnologías, al 31,4% de los jóvenes, entre 14 y 19 años, les parecería interesante recibir publicidad sobre el contenido que observan.

Para el 2016, la telefonía móvil llegaba casi a las 100 líneas por cada 100 habitantes (99,7) en el mundo, superando los 7.300 millones de líneas (ITU Statics, 2016). Mientras que en los países desarrollados alcanzaba las 126,7 líneas por 100 habitantes, en los países en vías de desarrollo se situaba en 94,1. A pesar de la relevante diferencia en la penetración de la telefonía móvil entre regiones desarrolladas y emergentes, la gran mayoría de las líneas (78,3%) está contratada en estas últimas, reflejando así la importancia que tiene este tipo de comunicación en

los países en vías de desarrollo, cuyos menores costes de despliegue frente a las comunicaciones fijas facilitan su rápida implantación.

Asia y Oceanía aglutinan el 57% de las líneas totales; en segunda posición se sitúa África, con el 13,2%, seguida de América Latina y el Caribe (9,6%), la Unión Europea (8,7%), el resto de Europa (5,7%) y Norteamérica (5,7%). Lo anterior ratifica la tendencia creciente de dependencia de la sociedad en el uso de las tecnologías de la información y las comunicaciones en las diversas áreas y facetas de la vida de los ciudadanos.

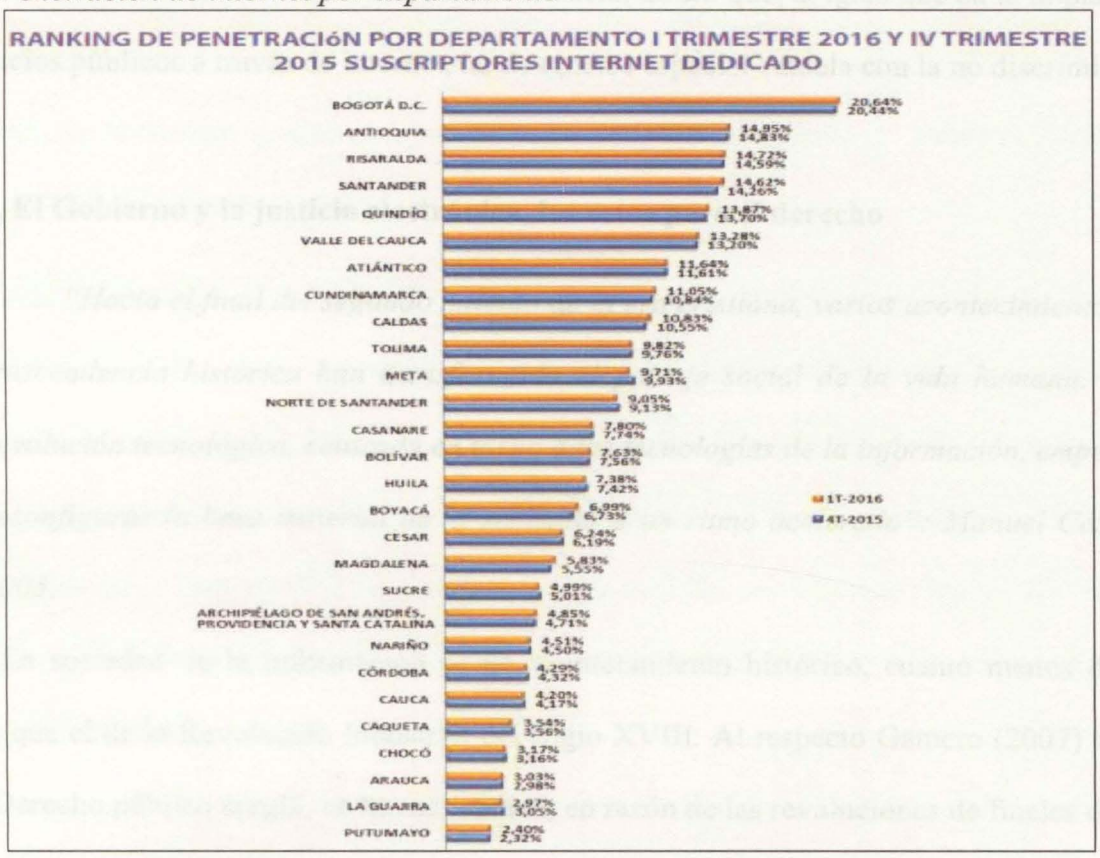
En Colombia, en cuanto al año 2013, se tenía un 108.3% de penetración de telefonía; el 42,2% de hogares reportaba computador de escritorio, portátil o tableta y el 35.7% acceso a internet. Un 47.5% de la población consultaba internet todos los días. Desde la perspectiva pública, el 100% de las entidades gubernamentales tenía presencia en un sitio web, ofreciendo al menos una plataforma de servicios a usuarios (Comisión Reguladora de Comunicaciones, en adelante: CRC, 2014).

En internet esencialmente se han ofrecido servicios para hacer consultas o denuncias por correo electrónico; así mismo, ha sido posible descargar, completar y enviar formularios (entre el 80% - 90% de administraciones). Sin embargo, la actividad de servicios de justicia ha estado muy reducida, con un modesto 1,3% (CRC, 2014).

Para el tercer trimestre de 2016, en el informe de penetración de tecnologías de la información de Colombia, por departamentos, se muestra la creciente demanda de conexiones a internet así:

Figura 2.

Penetración de internet por departamento



Nota: Tomado del boletín trimestral de las TIC hasta el primer trimestre de 2016. (MinTic, 2016, p 41.)

Pese al alto acceso y uso de internet, no debe olvidarse que no todas las personas quieren o pueden conectarse a internet y, hoy por hoy, la red reproduce e incluso intensifica, las pautas de marginalidad social no virtuales. Entonces, es necesario mostrar atención jurídica a la "*informarginalidad*", o al muro digital, social y territorial, así como a su obvia conexión con la implantación de la democracia y participación electrónicas.

Los sectores más marginados son los más necesitados de representación y de que el interés general se estructure sobre la base de sus necesidades. Estos sectores, precisamente, son los que

menos acceden a la red o lo hacen con menor eficacia; de ahí que, al igual que en la implantación de servicios públicos a través de internet, ha de tenerse especial cautela con la no discriminación.

3.1. El Gobierno y la justicia electrónica, los retos para el derecho

"Hacia el final del segundo milenio de la era cristiana, varios acontecimientos de trascendencia histórica han transformado el paisaje social de la vida humana. Una revolución tecnológica, centrada en torno a las tecnologías de la información, empezó a reconfigurar la base material de la sociedad a un ritmo acelerado": Manuel Castell, 2005.

La sociedad de la información es un acontecimiento histórico, cuanto menos de igual entidad que el de la Revolución Industrial del Siglo XVIII. Al respecto Gamero (2007) sostiene que el Derecho público surgió, en buena medida, en razón de las revoluciones de finales del siglo en mención y que dieron lugar al nacimiento de la Era Moderna; y hoy es posible que estemos en el momento en que el Derecho público deba readecuarse a esta nueva era: *Ubi cives, ibi ius*; es preciso que el Derecho lleve a cabo una tarea de inmersión en el sector.

Las TIC ya están aquí y han venido para quedarse (Cotino Hueso, 2007); como se ha visto, el grado de penetración y de usos avanzados de estas tecnologías es ya ineludible, al tiempo que no cesan de aumentar; y ello en modo alguno escapa al ámbito de los poderes públicos, la Administración y la Justicia. Aunque descubrir plenamente las enormes posibilidades del binomio Administración-TIC sea tarea de un prestidigitador, sí que es posible captar su importancia hoy y vislumbrar sus posibilidades en los próximos años.

Los poderes públicos van haciendo efectivas las diversas fases de implantación de la Administración electrónica, en especial las primeras (Gascó Hernández, 2001). De hecho, Colombia ha hecho un extraordinario esfuerzo de parametrización y racionalización de la implantación del Gobierno en línea.

Así sucedió con el incomparable esfuerzo hecho a través del Decreto 1151 del 14 de abril de 2008, que en su momento remitió al cumplimiento del "Manual para la implementación de la Estrategia de Gobierno en Línea". Dicho acto administrativo de carácter nacional —ya derogado— fue el precedente sobre el cual se han emitido los siguientes, que sucesivamente han reglamentado la materia, como el Decreto 2573 del 12 de diciembre de 2014, actualmente vigente. De este modo ha habido grandes avances y relevancia en el acceso y accesibilidad a la información de la Administración (primera fase).

De igual modo, se dan variadas formas de interacción básica (segunda fase), caracterizada en muy buena medida por la posibilidad de comunicación del administrado con la administración, aun por vías informales como el correo o las redes sociales. La tercera fase de interactuación en ambas direcciones (Administración-ciudadano), así como la cuarta (participación y democracia digital) ya están dando sus primeros pasos.

No en vano, para estas últimas fases se requería que las TIC se hicieran *carne social* entre la ciudadanía, y esto se ha conseguido no gracias a la e-administración, sino gracias al e-comercio, a la e-banca, empresas de vuelos y viajes y, ahora, gracias a la incursión de las redes sociales, que han hecho el trabajo de preparar a la ciudadanía para usar una e-administración que no ha estado realmente pensada para los usuarios. Ahora ya no hay excusas para dejar de hacer unos poderes públicos electrónicos realmente usables y usados por la ciudadanía.

Frente a antiguas promesas que podrían parecer idílicas, hoy en día ya no hay que convencer a nadie de la amplia lista de ventajas que la Administración electrónica puede reportar a la ciudadanía: mejora generalizada de los servicios y de la gestión de los asuntos y del conocimiento en las organizaciones públicas; reducción de los plazos; régimen de 7 días * 24 horas * 365 días al año; ahorro de tiempo y de traslados innecesarios; más y mejor información sobre los servicios y actuaciones; personalización de los servicios; simplificación y racionalización de los trámites; facilita la comunicación formal o informal del administrado y sus consultas; integración de servicios administrativos que son competencia de diversos agentes; menos documentación al ciudadano; mejor seguimiento y conocimiento del estado del procedimiento, así como la mejora del proceso de notificaciones y comunicaciones electrónicas.

A tales ventajas hay que añadir la enorme potencialidad de las TIC para la transparencia, el acceso a más y mejor información pública, así como la participación de los ciudadanos y los grupos en los que se integran la Administración y los procesos decisionales, en otras palabras, lo que hoy se denomina Gobierno Abierto (Cotino Hueso, 2013).

Ya en el ámbito más concreto de la Justicia, a las ventajas generales hay que añadir que las TIC permiten agilizar la tramitación de la oficina judicial, y realizar la gestión documental con mayor rapidez (Gamero Casado, 2012); también hacen viables las relaciones con terceros en plazos temporales brevísimos.

No cabe duda de que todo ello queda vinculado al derecho a un proceso sin dilaciones indebidas reconocido constitucional e internacionalmente. Al mismo tiempo, el uso de las TIC facilita las gestiones de los profesionales jurídicos; contribuye a reducir las necesidades de espacio requeridas por las oficinas judiciales. Igualmente, las nuevas herramientas ayudan a suprimir las

barreras territoriales y potenciar la igualdad, acortando distancias geográficas que en muchas ocasiones se tornan en verdaderos obstáculos para el acceso a la Justicia.

Del otro lado de la balanza, también es muy amplio el listado de las dificultades del gobierno en línea: el elevado coste de inversión, la desconfianza ciudadana por la seguridad, los problemas de interoperabilidad (conectividad de equipos y programas), las necesidades de formación del personal y de cambio de cultura administrativa; al igual que las dificultades de reasignación de los empleados públicos a nuevos puestos de trabajo, la existencia de recelos jurídicos, la desconfianza de los ciudadanos, la brecha digital y el agravamiento de la marginalidad.

A lo anterior, obviamente se añaden todos los problemas técnicos para satisfacer las exigencias jurídicas de la información y comunicación electrónicas: integridad, inalterabilidad, disponibilidad, trazabilidad, autenticidad o autenticación en origen y en destino, conservación, confidencialidad, no rechazo o no repudio en origen y en destino, y sellado de tiempo. Y no debe olvidarse que muchos de los problemas de la relación electrónica pueden tornarse en problemas de grave índole constitucional al repercutir en el derecho a la defensa y al debido proceso.

3.1.1. El paso del papel a lo digital es la oportunidad de garantizar el derecho a una buena Administración de justicia electrónica y mejorar su gestión. El e-expediente como instrumento que permite el análisis en la investigación penal.

Una expresión del reforzamiento de la posición jurídica del administrado se observa también con el reconocimiento del derecho a la buena Administración (Ponce Solé, 2001) y (Mallén T., 2004), directamente proyectada a la Administración de justicia. Se trata de un nuevo derecho fundamental reconocido desde 2000 en el artículo 41 de la Carta de los derechos

fundamentales de la Unión Europea, con valor jurídico desde la entrada en vigor del Tratado de Lisboa, en 2009; y pese a que la noción sea foránea, en Colombia no es materialmente extraña, pues aúna no pocas exigencias constitucionales. Se trata de un descriptor que integra diversas facultades y derechos del administrado.

Martínez Soria (2006) ha señalado que el gobierno electrónico posibilita y respalda el derecho fundamental del ciudadano a una buena Administración, y obviamente el de una buena Administración de justicia.

De este modo, la Administración electrónica o e-administración debe ser entendida como el uso de las TIC por parte de las Administraciones a fin de transformar sus estructuras, operaciones y, lo más importante, la cultura de la Administración. Lo anterior significa entender una Administración al servicio de los ciudadanos, y no lo contrario; es concebir una Administración eficiente, eficaz, responsable, abierta, transparente, participativa, respetuosa de la ley y garante de los derechos de los ciudadanos, como lo señala Cotino Hueso (2008), para quien las TIC ya dejaron de ser inminentes sino que se encuentran involucradas en el día a día de un número de ciudadanos cada vez más creciente, y el derecho debe corresponder a tal momento histórico.

3.1.2. El big data como ejemplo de la necesidad de reencausar la investigación criminal.

En el marco de la utilización de las TIC, en los últimos años, han surgido herramientas de análisis masivo de información al interior de las organizaciones de todo tipo, incluidas las propias administraciones gubernamentales; la combinación entre servicios, herramientas, información, datos (muchos de estos privados), y las nuevas técnicas de gestión de los mismos, como pueden ser las que utilizan *big data*, ocasionan situaciones que pueden poner en riesgo a Gobiernos,

Administraciones, ciudadanos, empresas, entre otros; por ende, su previsión debe ser un elemento en el marco del desarrollo de las competencias de cada Administración.

Tras el inicio del tercer milenio, las organizaciones privadas y públicas tienen acceso a la información de una forma sin precedentes.

Los datos, que se generan a través de un sinnúmero de aplicaciones y de sistemas que sirven como soporte a los procesos de negocio, servicios, transacciones comerciales y redes sociales, entre otros, se encuentran no sólo en formatos estructurados y en bases de datos tradicionales, sino también en forma de imágenes, voz, posicionamiento geográfico, etc. (Salvador, 2014).

Estos datos a grandes volúmenes solo son manejables a través de la tecnología que involucra *big data,* según se explicitó en acápites precedentes.

3.1.3. La afinidad entre la e-administración y la e-justicia en sus definiciones y su regulación, una referencia de la necesidad de normas en Colombia para regular la materia.

Como ya se mencionó, la e-justicia es un ámbito específico de la e-administración; entre las diversas definiciones de administración electrónica, prefiero la siguiente:

> [...] es el uso de las tecnologías de información y comunicaciones que realizan los órganos de la Administración para mejorar los servicios e información ofrecidos a los ciudadanos, aumentar la eficiencia y la eficacia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación de los ciudadanos [...] (Chile, Sec. Gral. Presidencia, 2008 p. 2)

La afinidad entre la e-administración y la e-justicia es innegable y va más allá del concepto mismo, llegando al régimen jurídico aplicable. En España, por ejemplo, el marco jurídico de la e-justicia es ya muy amplio y diferenciado del de la e-administración. Especialmente, cabe subrayar la dualidad de las dos amplias leyes reguladoras: la Ley 11/2007 de e-administración y la Ley 18/2011 reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

La ley de e-justicia posterior emula en ocasiones, de manera muy evidente, al punto de la transcripción a su matriz de e-administración, especialmente en cuestiones de sede, firma, registros o notificaciones electrónicas. Pero también es cierto que presenta diferencias, como recuerda la exposición de motivos de la norma reguladora del uso de las tecnologías de la información y la comunicación en la Administración de justicia, Ley 18/2011:

> La Administración de Justicia presenta características que la diferencian de las restantes Administraciones públicas. En primer lugar, por la propia naturaleza de la función que la Administración judicial tiene atribuida, ya que se trata de un poder del Estado distinto del poder ejecutivo, en el que se encuadran las Administraciones públicas que, además, debe satisfacer un derecho fundamental[...] (p. 3)

Entre los muchos instrumentos y normas de derecho comparado español, cabe mencionar: la Carta de Derechos de los Ciudadanos ante la Justicia, del 16 de abril de 2002 (Portal de Justicia de la comunidad de Madrid, s.f.); el Real Decreto 937/2003 de modernización de los archivos judiciales; el Acuerdo del Pleno del Consejo General del Poder Judicial, del 20 de septiembre de 2006, de creación de ficheros de carácter personal dependientes de los órganos judiciales, y el Real

Decreto 95/2009, del 6 de febrero, que regula el Sistema de registros administrativos de apoyo a la Administración de Justicia.

La Orden del Ministerio de Justicia del 19 de julio de 1999 aprobó el Proyecto de Informatización, en cuyo ámbito se han desarrollado medidas diversas como la creación de INFOREG —aprobada en 2001 y modificada por Orden JUS 1468/2007, de 17 de mayo, sobre impulso a la informatización de los registros civiles y digitalización de los archivos— también se estableció el Programa Registro Civil en Línea dentro del Plan Avanza (Agenda digital para España, s.f.). Es procedente destacar la Ley 13/2009, del 3 de noviembre, de reforma de la legislación procesal para la implantación de la nueva Oficina Judicial (LINOJ). Además, se encuentra el Acuerdo, del 15 de septiembre de 2005, del Pleno del Consejo General del Poder Judicial (en adelante: CGPJ), por el que se aprueba el Reglamento 1/2005, concerniente a los aspectos accesorios de las actuaciones judiciales.

Igualmente, está el Plan de Modernización de la Justicia, aprobado el 11 de noviembre de 2008 por el Pleno del CGPJ (Poder Judicial de España, s.f.a) y el Plan Estratégico para la Modernización del Sistema de Justicia (2009-2012), aprobado en Consejo de Ministros (Ministerio de Justicia, 2009). Así mismo, en 2012, se aprobó el Plan de acción de la Administración de Justicia 2012-2015 (España, Min Justicia, 2012). También se encuentra el Real Decreto 84/2007, de 26 de enero, sobre la implantación en la Administración de Justicia del sistema *Lexnet*, que se incorpora por Ley 41/2007, del 7 de diciembre, sobre Reforma del Mercado Hipotecario, que modificaba el Acuerdo del 15 de septiembre de 2005, del Pleno del CGPJ.

La opción colombiana, igualmente legítima, es la de partir de un régimen jurídico común, el establecido por la Ley 1437 de 2011 —Código de Procedimiento Administrativo y de lo

Contencioso Administrativo (en adelante: CPACA)— sin perjuicio de señalar las oportunas especialidades de la e-justicia, que se presentarán en el título correspondiente a la estrategia.

3.1.4. Algunas referencias sobre la evolución en Europa, España y Colombia y la necesidad de normas que articulen la efectividad de la Administración de justicia electrónica.

La e-justicia ha tenido un gran impulso como objetivo de la Unión Europea (Cerrillo Martínez, 2007). Se ha articulado en lo que antiguamente se denominaba Tercer Pilar y que, tras el Tratado de Lisboa de 2007, es la política específica de creación de un espacio de libertad, seguridad y justicia, con competencias compartidas con los Estados miembros (Cotino Hueso, 2003).

La relativa independencia de esta política de e-justicia se inicia en 2003, desde la Conferencia conjunta "*Internet strategies and e-justice in Europe*" (Estrategias de internet y e-justicia en Europa), que se celebró con el Consejo Europeo (en adelante: Consejo) en 2003; posteriormente, inició labores el Grupo Informática Jurídica (justicia en línea) del Consejo sobre la base del Informe del 5 de junio de 2007. A partir de este documento se profundizó en el fomento de la justicia en línea y se planteó la utilización de las TIC para las comunicaciones entre los órganos judiciales y las partes (European Council, 2007, p. 44). Este avance desembocó en la estrategia europea en esta materia, plasmado en el Plan de Acción Plurianual 2009-2013 relativo a la Justicia en red europea del Consejo Europeo (Consejo 2008).

Así mismo, el Consejo Económico y Social Europeo recordó la necesidad de respetar el valor fundamental de la justicia más allá de la eficacia, haciendo hincapié en la necesaria seguridad

que debe acompañar el proceso de implantación de las TIC en la Justicia. Estos documentos, junto con el Programa de Estocolmo (Comisión Europea, 2010) constituyen hasta hoy la base del desarrollo de las múltiples medidas de e-justicia europea.

Estos proyectos pretenden la desmaterialización (Arangüeña Fanego, 2010), de los procesos en el ámbito de la cooperación judicial civil y en las medidas de comunicación judicial electrónica previstas en el procedimiento monitorio europeo (Parlamento Europeo y Consejo, 2006) y los procesos de escasa cuantía (PE y Consejo, 2007).

Cabe señalar que el Portal Europeo de e-justicia, al día de hoy, afirma que "está pensado para ser en el futuro una ventanilla única en el ámbito de la justicia" (Comisión Europea, s.f.).

En España, el tratamiento jurídico de la e-administración se inició con la Ley 30/1992, de 26 de noviembre (ya derogada) cuyo artículo 45 introdujo la posibilidad de que "Las administraciones públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y el ejercicio de sus competencias".

Desde entonces se dieron sucesivas reformas, muchas normas reglamentarias sectoriales, estatales y regionales hasta la Ley 11/2007, de 22 de junio (hoy derogada), de acceso electrónico de los ciudadanos a los servicios públicos cuyo acertado lema no fue otro que el de pasar del "podrán" al "deberán". Así, la e-administración dejó de ser una posibilidad para ser una obligación jurídica para la Administración y un derecho de la ciudadanía.

En el ámbito de la Justicia, el pistoletazo de salida se dio con la Ley Orgánica 16/1994, de 8 de noviembre, para introducir la posibilidad de utilizar medios electrónicos.

Entre 2002 y 2004 se dio un pacto político por la modernización de la Justicia que generó muchas actuaciones y regulaciones. Así, se impulsó el reconocimiento de la plena eficacia y validez de los documentos electrónicos; se regularon los archivos y registros judiciales; se digitalizaron los registros civiles, se actuó respecto de la interoperabilidad y compatibilidad de medios electrónicos dentro de la Justicia. Destacó la dotación de firma electrónica a jueces y magistrados para proporcionar identidad digital a los titulares de los órganos jurisdiccionales y, de forma decisiva el llamado "Punto Neutro Judicial" (Poder Judicial de España, s.f.).

Aunque con orígenes en 2000, desde 2009 se articuló la primera red extensa de comunicaciones que enlazaba a todos los órganos judiciales de España; lo más importante es que sobre ella se desarrolló una serie de enlaces que le permite a los órganos judiciales conectarse directamente con las bases de información de organismos públicos y privados, necesarios en la tramitación judicial. Hoy en día es un portal que facilita la gestión procesal y que permite el acceso a millones de documentos de decenas de administraciones y registros.

De igual modo, es especialmente destacable el sistema *Lexnet* regulado por el ya derogado Real Decreto 84/2007, de 26 de enero (de Hoyos Sancho, 2008). Se trata del sistema informático de telecomunicaciones para la presentación de escritos y documentos, el traslado de copias y la realización de actos de comunicación procesal por medios telemáticos; una plataforma tecnológica que permite el intercambio seguro de documentos y escritos procesales entre las partes.

El Plan de Modernización de la Justicia, del 11 de noviembre de 2008 por el Pleno del CGPJ (Poder Judicial de España, s.f.a.) y el Plan Estratégico para la Modernización del Sistema de Justicia (2009-2012) de septiembre de 2009 impulsaron la implantación del expediente judicial electrónico (España, Ministerio de Justicia, 2009) .

Asimismo, se aprobó la Ley 13/2009, de 3 de noviembre, para la implantación de la Nueva Oficina Judicial que permite las pujas electrónicas en subastas judiciales o el uso de medios telemáticos, informáticos y electrónicos en sustitución de las publicaciones en boletines oficiales; y la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

En Colombia, la Sala Administrativa del Consejo Superior de la Judicatura (en adelante CSJud) incluyó las TIC como uno de los factores críticos en el Plan de Desarrollo 2011-2014, que contempla el Plan Estratégico Tecnológico para la Rama Judicial Colombiana (CSJud, 2012); así mismo, renovó sus compromisos del Plan Nacional de las TIC 2010-2019.

En el país también se cuenta con la iniciativa Vive Digital del Ministerio de las TIC, todo con el objetivo de que "[...] la prestación del servicio público de la Justicia se realice en condiciones de accesibilidad, celeridad y excelencia, con altos niveles de calidad y transparencia y con un adecuado sistema de rendición de cuentas [...]", bajo los siguiente ejes: sostenibilidad, coordinación con las iniciativas nacionales e internacionales del gobierno en línea, apoyo a la implementación de la oralidad, auditoría de sistemas, creación de un grupo de coordinación y de seguimiento, seguridad y calidad de la información, enfoque de género y fortalecimiento de la infraestructura TIC.

Finalmente, y de la mayor importancia, como se mencionó, se aprobó la Ley 1437 de 2011 (CPACA) dentro de la cual se regula —en sus artículos 53 a 64— la utilización de medios electrónicos en el procedimiento administrativo; entre otras cuestiones, cabe destacar que

incorpora la posibilidad de contar con un expediente judicial electrónico en razón del artículo 186[9] y se establece una obligación para su implantación a la Sala Administrativa del Consejo Superior de la Judicatura en cinco años (2016)[10].

De conformidad con el principio de coordinación, corresponde al Consejo Superior de la Judicatura y a las autoridades administrativas competentes, como el Ministerio de Tecnologías de la Información y las Comunicaciones (en adelante: MINTIC), actuar de manera coordinada y ello se realiza a través de la puesta en marcha del Plan de Gobierno en Línea liderado por dicha cartera, a fin de que los esfuerzos realizados tengan sus mejores resultados.

En la sección correspondiente a la estrategia se pondrán de presente otros elementos del marco jurídico colombiano en cuanto a gobierno y justicia electrónicos.

3.2. La justicia electrónica y las investigaciones electrónicas, su proyección como elemento esencial del análisis en la investigación penal. Lo que hay y lo que nos falta.

En el marco de las obligaciones señaladas para el Ministerio TIC, a partir del principio de coordinación armónica de las diferentes autoridades, en cuanto al desarrollo de programas y proyectos que incorporen TIC, se cuenta con un Nodo de Innovación en Justicia, conformado por

---

[9] "…todas las actuaciones judiciales susceptibles de surtirse en forma escrita se podrán realizar a través de medios electrónicos, siempre y cuando en su envío y recepción se garantice su autenticidad, integridad, conservación y posterior consulta, de conformidad con la ley. La autoridad judicial deberá contar con mecanismos que permitan acusar recibo de la información recibida, a través de este medio".

[10] Según el artículo 186, la Sala Administrativa del Consejo Superior de la Judicatura, "…adoptará las medidas necesarias para que en un plazo no mayor de cinco (5) años, contados a partir de la vigencia del presente Código, sea implementado con todas las condiciones técnicas necesarias el expediente judicial electrónico, que consistirá en un conjunto de documentos electrónicos correspondientes a las actuaciones judiciales que puedan adelantarse en forma escrita dentro de un proceso".

diversos grupos, a saber, academia, Gobierno, industria, usuarios, que permitan el desarrollo, uso y apropiación de TIC en la Administración de justicia.

Bajo este presupuesto, y haciendo un ejercicio de vigilancia tecnológica, el nodo ha encontrado que diversos países han implementado programas tendientes al desarrollo de una Administración de justicia electrónica

Por ejemplo, el documento Agenda Estratégica de Innovación Nodo Justicia (Min TIC, 2014) señala que, en Perú, el sitio del Poder judicial les da la posibilidad a los ciudadanos de acceder a toda la información relativa a la transparencia de la institución.

Los usuarios de ese sitio web pueden consultar informes de asignación y ejecución de recursos, así como de gestión administrativa, cantidad de personal, costos de operación y reportes de contratos administrativos, de bienes y servicios. En el sitio también se publican los concursos abiertos, licitaciones públicas, adjudicaciones directas y planes anuales; igualmente, cuenta con las hojas de vida de los jueces y magistrados, las cuales pueden ser consultadas por los usuarios.

Acerca de lo que sucede en España, el documento en referencia señala que el Punto Neutro Español posibilita la consulta de información entre las diversas plataformas de las comunidades autónoma, y las diferentes entidades del Estado, incluyendo los propios órganos judiciales y el Centro de Documentación Judicial (en adelante: Cendoj).

En ese mismo sentido, el documento del MinTic señala que sistema Push de Brasil es una herramienta de consulta y seguimiento de los procesos judiciales, abierta y gratuita; pero no solo es de consulta, sino que el interesado puede suscribirse para recibir información, vía correo electrónico, acerca de los procesos que le conciernan.

A modo de conclusión, en la publicación Nodo de Justicia del MinTic se determinaron las siguientes líneas para ser desarrolladas:

1. Justicia en línea.
2. Arquitectura de la información.
3. Uso de las TIC, para educación, formación y gestión del cambio en Justicia.
4. Interoperabilidad
5. Uso TIC en la investigación judicial y criminalista.

Para esto determinaron la necesidad de:

1. Reconocimiento del estado actual de los servicios en la e-justicia.
2. Identificación de los principales actores.
3. Primera etapa de acercamiento y entrevistas con los principales actores.
4. Presentación individual de la Agenda Estratégica de Innovación a los actores principales entrevistados en la primera etapa.
5. Consolidación de las observaciones y sugerencias de los actores entrevistados.

En la primera fase de desarrollo, según se informa en el aludido documento de 2014, se habían realizado las siguientes actividades: Revisión del Plan TIC de la Rama Judicial para el período 2006 – 2010; Identificación de avances reglamentarios y tecnológicos impulsados por la Sala Administrativa del CSJud durante el período 2006 - 2010, pertinentes para la implantación de la estrategia e-justicia adoptada formalmente por esta Sala en sesión del 22 de septiembre del 2009.

Igualmente, se contempla la revisión de experiencias nacionales e internacionales exitosas en el uso de TIC y en la Administración de justicia como la realización del "Foro E-Justicia: Las Tecnologías de la Información y las Comunicaciones para el mejoramiento de la Administración de justicia", efectuado el 25 de noviembre 25 de 2009; formulación de recomendaciones en temas

reglamentarios, tecnológicos y organizacionales para la implantación efectiva de la estrategia e-justicia en el período 2010-2014 con perspectivas al 2019; "Concurso Aplicación de las TIC para el mejoramiento de los servicios de Justicia"; y el "Foro virtual: ¿Cuáles servicios de la Administración de justicia le gustaría recibir haciendo uso de las TIC?".

El mismo documento señala la realización de un conjunto de actividades prioritarias en una segunda fase, así:

> [...] Formulación del Eje Justicia en el nuevo Plan TIC, ampliado a todas las instituciones del Sector Justicia (GEL) y de otros sectores relacionadas con el quehacer judicial; Revisión de cada una de las estrategias institucionales respecto a TIC, su grado de avance y sus perspectivas para el período 2010 - 2014 con visión al 2019; Definición consensuada de una Agenda inter-institucional, que demande esfuerzos coordinados durante el período; Formulación conjunta de Objetivos y Metas de la Agenda interinstitucional, en coordinación con el Ministerio de TIC y el DNP; Apoyo a las instituciones en la formulación del Plan TIC en lo relativo a la Agenda inter-institucional (II) y recomendaciones para su Plan TIC institucional; Elaborar propuestas de marco regulatorio necesario para el uso de las TIC en la justicia [...]

Finalmente, es importante resaltar que cualquier proceso integral de incorporación de tecnologías en la Administración de justicia deberá contar con la participación directa de las diferentes jurisdicciones como lo son la ordinaria, contenciosa administrativa, constitucional, la penal militar; así como la de las comunidades indígenas y la jurisdicción de paz. Igualmente, se requiere la intervención de entidades como la Fiscalía General de la Nación, el Ministerio Público,

el Consejo Superior de la Judicatura, y diversas autoridades administrativas y árbitros. También deben participar abogados, ciudadanos y habitantes del país en general.

El Plan Nacional TIC 2010 – 2019 del Ministerio de Justicia ha trabajado en la implementación del proyecto "e-Justicia", incorporando a la Rama Judicial, la Fiscalía General de la Nación, la Policía Nacional, el Instituto Nacional Penitenciario y Carcelario (en adelante: Inpec), la Defensoría del Pueblo, la Procuraduría General de la Nación, las notarías, las cámaras de comercio, entre otros, para procurar una infraestructura tecnológica de TIC homogénea e interconectada, a fin de garantizar su interoperabilidad y un mejor funcionamiento de la misma.

Por lo anterior, el plan referido define cuatro ejes temáticos:

- Eje 1. Modelo de expediente electrónico.
- Eje 2. Justicia en red.
- Eje 3. Gestión de la información.
- Eje 4. Gestión del cambio.
- Eje 5. Uso de las TIC para la formación judicial y ciudadana, así mismo se han venido disponiendo los recursos financieros para este fin.

Así las cosas, cualquier proceso de desarrollo e implementación tecnológica que quiera hacer la Fiscalía General de la Nación debe estar debidamente coordinado con las autoridades que conforman las ramas del poder público y los órganos de control.

4. La estrategia de ciberseguridad como espina dorsal de la gestión y análisis en las investigaciones penales por medio de las TIC

4.1. Análisis del caso Estonia

El ejercicio de actividades públicas y privadas, teniendo como base las TIC, acarrea nuevos elementos, entre ellos uno de vital importancia: la seguridad, y de manera específica la ciberseguridad. Un ejemplo de ello, en el tema objeto de la presente investigación, es el denominado caso Estonia: un ataque contra los sistemas de información de entes públicos y privados que hizo colapsar por varios días el normal funcionamiento de uno de los Estados más conectados a la red en todo el mundo.

En ese orden de ideas, aparecen dos elementos iniciales, por un lado, la utilización de TIC en la Administración pública y, por otro, la afectación a la seguridad y defensa nacionales de un Estado, ocasionada por un ataque a la estructura o información que soporta esa utilización.

Frente a esto, se pone de presente la necesidad de determinar cómo se desarrollan e incorporan los elementos de la guerra en el ciberespacio cuando se ataca una infraestructura crítica como la de la administración general del Estado.

Me permito iniciar el presente escrito con las palabras que mejor han descrito la amenaza de la ciberguerra y estas son las de Richard Clarke:

"*La ciberguerra ha empezado. Adelantándose a las hostilidades, las naciones están ya "preparando el campo de batalla". Están 'hackeando' sus redes e infraestructuras unas a otras, dejando puertas traseras y bombas lógicas: ahora, en tiempos de paz. La vigencia*

de la ciberguerra, el hecho de que sea algo en desarrollo, que difumina los límites entre la paz y la guerra, añade una dimensión de inestabilidad nueva y peligrosa". Clarke, R. (2011)

El presente estudio no es otra cosa que un fiel ejemplo de la alarma de Clarke (2011). De manera inicial el lector encontrará un análisis de lo sucedido en el llamado caso 'Ciberataque a Estonia'; se señala el evento en particular que ocasionó que un conjunto de servidores y redes públicas y privadas colapsaran trayendo como resultado la denegación de servicios a los usuarios por medios electrónicos. Posteriormente, se explicarán los componentes de la operación cibernética y la respuesta frente a dicho incidente, con el detalle de los elementos que se requieren para hacer frente a ataques de este tipo. También se hará un análisis de los aspectos que intervienen en la utilización de TIC por parte de la Administración pública, de manera particular hasta el uso de aplicaciones de análisis masivo de información o de *big data*; por último, se señalarán los instrumentos con los que cuenta el Estado colombiano para hacer frente a ataques ocasionados contra la infraestructura crítica de la Administración pública, y además se darán unas conclusiones.

4.1.1. Caso de estudio –Estonia– antecedentes

Para el año 1989, la desintegración de la Unión Soviética llevó a que algunas de las repúblicas que la componían se apartaran de Moscú, entre ellas Estonia, a través de su capital Tallin, ciudad que había sido obligada a hacer parte de aquella superpotencia tras ser liberada de los nazis por el Ejército Rojo, hecho conocido como "la gran guerra patria" (Richard, 2011, p. 368).

Lo anterior ocasionó que ni este ejército, ni el Partido Comunista de la Unión Soviética, quisieran que dicha liberación fuera olvidada por los estonios; por esto, en la ciudad de Taillin, se construyó la estatua de un soldado del Ejército Rojo y la regla era colocar dicha estatua sobre las tumbas de los soldados comunistas.

Las estatuas tenían un alto significado para los rusos, pero también para quienes habían sido liberados; no obstante, el sentido que le daban unos y otros era diferente.

Luego de terminar la Guerra Fría, se declaró la independencia de Estonia y la mayoría de sus ciudadanos quería eliminar todos los símbolos de la opresión que se había vivido al haber tenido la obligación de ser parte de la Unión Soviética; por lo cual se aprobó la Ley de Estructuras Prohibidas, en ella se estableció, entre otras cosas, el derribo de estatuas como la del soldado del Ejército Rojo, que se alzaba en diferentes ciudades.

Esto ocasionó que Moscú protestara, argumentando que era una profanación a los hombres que yacían bajo las estructuras de bronce; entonces, con el ánimo de no generar un problema diplomático, el presidente de Estonia vetó la Ley; tal decisión alimentó la opinión del pueblo, el cual se dividió en dos bandos: por un lado, los estonios de origen ruso y, por otro, los nacionalistas estonios, los primeros querían que se mantuvieran dichos símbolos, los segundos que se derribaran. Al final estalló una confrontación que trasciendió al ciberespacio (Richard, 2011, p. 368).

4.1.2. Estonia, la red y el ataque.

Estonia es un Estado conectado (Informe Freedom House, 2014), esto lo convirtió en un objetivo directo para realizar un ciberataque, y a raíz de los hechos señalados en el apartado anterior lo recibió, en 2007, específicamente a los servidores donde estaban alojadas las páginas

web más utilizadas del país. La agresión fue originada en una avalancha de solicitudes de acceso y el bloqueo de muchas de estas; no se podía acceder a los servidores, a los bancos, a los periódicos, ni a muchos servicios electrónicos del Gobierno.

El tipo de ataque no era otro que un *ataque distribuido de denegación de servicios* también conocido como DDOS. Fue una programación anticipada con el objetivo de sobrecargar y bloquear la red a raíz del gran volumen de información; para lograr una incursión de esta clase se utilizan miles de ordenadores que envían solicitudes para conectarse a un mismo punto de conexión de internet.

En este caso se utilizó un *botnet*, es decir, un conjunto de computadores robots contralados de manera remota para que cumplan una orden específica y conectarse a un mismo punto para colapsarlo. Una característica muy importante de este tipo de ataque es que los propietarios de los computadores no se enteran que hacen parte de un *botnet* o mejor dicho de que son simples cumplidores de órdenes.

Para el caso específico la situación fue ocasionada porque, en días anteriores, los usuarios de los computadores empleados para el ataque, sin saberlo, descargaron el software necesario para convertirse en un *zombi*; ello a través de algún correo electrónico que abrieron, una página descargada, entre otros métodos similares. Así, este programa pudo buscar otros computadores para infectar a través de la técnica de gusano y conseguir el mayor número de computadores *zombi*.

Se dice que ha sido el mayor ciberataque de la historia; participaron más de un millón de computadores, comercio, comunicaciones, bancos y la propia Administración. Fue una situación extrema que duró varios días, al punto que se escaló al Consejo del Atlántico Norte, máxima autoridad de la OTAN, que conformó un grupo ad-hoc para dar respuesta a este incidente.

Se emplearon técnicas de rastreo, se siguieron las conexiones atacantes y luego las vigilaron hasta determinar el momento en que las máquinas se comunicaban con la matriz. Con tales medidas, Estonia llegó a asegurar que los ataques provenían de Rusia y el código empleado se había escrito en alfabeto cirílico[11]. Como consecuencia de ello la OTAN creó en Tallin un centro de Ciberdefensa que se inauguró en 2008 (El País, 2009).

4.1.3. Componentes de la operación cibernética en el caso Estonia.

Inicialmente el equipo ad-hoc, creado por la OTAN, realizó un análisis de 'Conciencia situacional cibernética', entendido como "la representación mental y comprensión de los objetos, eventos, gente, estados de los sistemas, interacciones, condiciones ambientales y cualquier otro tipo de factores de una situación específica que puedan afectar al desarrollo de las tareas humanas, bien sean complejas o dinámicas" (Endsley, M. R., 2000). Esta conciencia permite tener el conocimiento inmediato del ciberespacio amistoso, adversario y otra información pertinente relativa a las actividades que se desarrollan en este ámbito y en el espectro electromagnético; se obtiene con percepción, comprensión y proyección.

El objetivo principal del equipo ad-hoc para la respuesta al incidente de Estonia era mantener la confidencialidad, integridad y disponibilidad de la información y los servicios, así como los sistemas de información y comunicaciones, a partir de las actividades de inteligencia, fundamentales en el levantamiento y actualización de un estado de conciencia situacional

[11] Este alfabeto está basado en el alfabeto griego con caracteres del alfabeto glagolítico y con sonidos exclusivamente eslavos, inventado en el siglo X por un misionero del Imperio bizantino en el Primer Imperio búlgaro.

cibernético; actuación que para el caso puntual fue realizada por los expertos en ciberseguridad de la OTAN.

Es importante referir que en este caso se evidenció el cumplimiento de las características propias de las batallas que se desarrollan en la 'Quinta dimensión', a saber, indefinición del estatus del oponente, no se sabía quién era; lucha asimétrica; tenían capacidad; largo empleo de instrumentos; las maniobras fueron a base de información. El punto de partida del combate librado fue el movimiento de una estatua, no cualquiera, una que tenía un significado diferente para cada uno de los actores, es decir, no fue el ánimo del crimen, ni del terrorismo, ni del espionaje, sino de los hackers que a través de computadores zombis manifestaron su total rechazo al movimiento de las estatuas del soldado del Ejército Rojo.

Los hackers utilizaron técnicas de exploración de vulnerabilidades, tras las cuales desarrollaron, sin autorización legal, acciones orientadas a: acceder a computadores de diversos tipos de usuarios; preparar dichos computadores como una red *botnet* o zombi; enviar solicitudes al mismo tiempo y durante un periodo determinado con el objetivo de bloquear los sistemas y servicios ofertados por el comercio, los bancos, y la Administración pública de Estonia.

4.1.4. La respuesta frente al incidente de Estonia.

Como se mencionó, el Gobierno de Estonia, entre otras actividades de reacción, llevó la emergencia a instancias de la OTAN, tras lo cual se creó un equipo de respuesta ad- hoc, cuyas actividades, a pesar de no estar escritas en ese momento, se centraron en las siguientes ofensivas (de explotación) y defensivas:

Las actividades ofensivas tienen el objetivo de irrumpir, negar uso, degradar, corromper, destruir sistemas computacionales o informaciones en equipos y redes de computadores conducidos en el espectro magnético o en equipos y se pueden direccionar a los sistemas con armas; además de que emplean técnicas de disimulación, amparadas legalmente, que se integran con la inteligencia.

Dentro de esas acciones de ataque, los especialistas de la OTAN pensaron en la realización de ingeniería social; ataques a software de aplicaciones, a hardware y ataques por inserción de malware; así como negación de servicios y de servicios de distribución; secuestro URL, así como al sistema inalámbrico; desfiguración de página, fuerza bruta, interceptación de tráfico, e inyección SQL; amenaza persistente avanzada y ataques *zero-day*.

Se determinó que lo mejor era la realización de actividades de explotación para búsqueda o recolección con el fin de obtener datos, ello a través de redes sociales, acompañamiento en internet, repercusión de las operaciones, así como acompañamiento a hackers oponentes, y seguimiento de noticias, sitios web de divulgación de ataques y neutralidades; esto se acompañó de acciones de desinformación, datos de vulnerabilidades del oponente y creación de páginas falsas.

Se realizaron actividades defensivas, entiéndase por estas la protección para neutralizar ataques, estas son permanentes; su objetivo principal es la detección, identificación y respuesta a acciones realizadas por el oponente, con acciones de contrainteligencia, revisión de redes, restablecimiento, reconstrucción de redes degradadas o comprometidas.

Por lo cual se creó el equipo ad-hoc de gestión de riesgos; se efectuaron actividades de análisis del incidente de seguridad y se llevó a cabo el tratamiento por los expertos; también se dio soporte a la recuperación y coordinación.

4.1.5. Lo que se necesita para hacer frente a casos similares a Estonia.

Es importante el diseño de una estrategia de ciberseguridad por parte de los Estados; por ello, hay que señalar algunos de los elementos que fundamentarán la misma. Uno de los pilares es la colaboración entre los diversos actores sociales, el Estado, la industria, la academia, entre otros, es decir, la relación entre lo público y lo privado cobra un papel esencial en el diseño e implementación de estrategias de ciberdefensa.

Otro de los elementos fundamentales es la capacidad tecnológica, que a su vez debe estar nutrida por una fuerte política de desarrollo en ciencia y tecnología por parte de las administraciones; para finalizar, la política de ciberseguridad debe involucrar a todos los actores.

Cualquier estrategia deberá contar con unos niveles propios de organización, esto es, un nivel político o estratégico, uno operacional y otro táctico, cada uno de estos independiente pero relacionado de manera integral con los otros, esto no significa otra cosa que la necesaria relación entre unos y otros.

No se puede dejar de lado que esto trae consigo unos desafíos entre los que podríamos recordar: capacitar los recursos humanos, incrementar proyectos, perfeccionar la investigación científica, realizar acciones multidisciplinares, la generación de nuevas capacidades en el sector defensa entre otras.

Debo resaltar que la actuación cibernética en el nivel político estratégico se caracteriza porque los objetivos perseguidos son políticos; es fundamental la obtención de inteligencia, así mismo la participación de los diferentes niveles de la Rama Ejecutiva del poder, especialmente la intervención de varios ministerios.

Esta actuación se realiza desde tiempos de paz, hay un empleo de nivel tecnológico alto, se desarrolla dentro de un contexto de una operación de inteligencia compleja, es de duración prolongada.

De este modo, una estrategia de defensa cibernética se deberá fundamentar en el principio de efecto, esto es, los efectos frente a las acciones que se desarrollen en el ciberespacio deben representar una ventaja estratégica, operativa o táctica, sin importar que estos no sean cinéticos.

También debe estar presente el principio de disimulación: la defensa cibernética debe adoptarse a partir de la disimulación en el ciberespacio, de tal manera que el rastreo de las acciones ofensivas y exploratorias que se realicen en contra de los sistemas de TIC del oponente sean muy difíciles. Se busca no permitir la autoría y el punto de origen.

Igualmente, está el principio de rastreabilidad: en su mayoría, las acciones que se desarrollan en el ciberespacio están determinadas por el movimiento o la manipulación de los datos que se pueden registrar en los sistemas TIC.

A lo anterior se suma el principio de adaptabilidad: una de las características del ciberespacio es la mutabilidad, en virtud de la cual es exigible, a partir de este principio, que las medidas adoptadas detecten acciones cibernéticas ofensivas y exploratorias de los sistemas de TIC, a partir de la adaptación a las innumerables formas que adquieran.

Todo esto es posible a partir de la consideración de contar con: capacidades operativas, gestión de riesgos, conciencia situacional, defensa activa, respuesta rápida, forense digital, prueba de artefactos cibernéticos y ataque cibernético, inteligencia cibernética, sistemas de información y comunicaciones (en adelante: SIC), gestión de incidentes de red.

Así mismo, se deben tener capacidades estructurales, seguridad de la información y comunicaciones, al igual que protección de las infraestructuras críticas, movilización, gestión de la crisis, gestión de las personas, asociaciones estratégicas y capacidad de resiliencia.

4.2. El cumplimiento de la misión institucional por medio de las TIC y la necesidad de enmarcar la estrategia de ciberseguridad a partir de la implementación de la estrategia de gobierno electrónico.

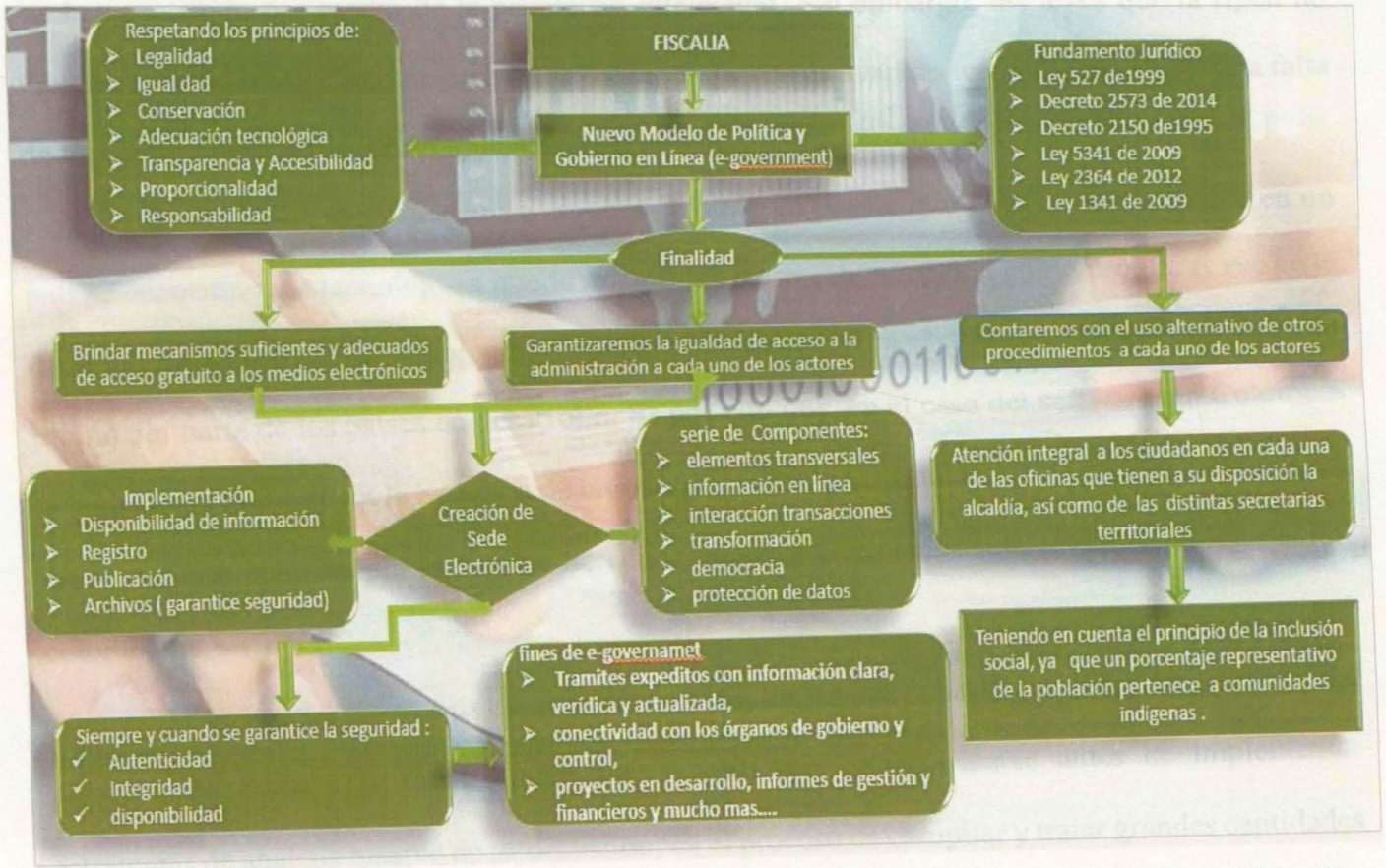


Figura 3: Política y gobierno en línea – e-gobierno, tomada de una presentación elaborada previamente por el autor.

4.2.1. La necesidad de una estrategia de ciberseguridad en la Fiscalía General de la Nación.

4.2.1.1. Ciberseguridad y big data en la Administración pública colombiana, especial referencia a la necesidad de proteger el resultado de los análisis que se dan en el marco de las investigaciones penales.

Existen varios puntos legales neurálgicos a la hora de compilar, almacenar y tratar grandes cantidades de información, es por ello que los creadores de tecnologías capaces de hacer *big data* las han protegido por medio de la propiedad intelectual. Sin embargo, las leyes que la rigen no fueron concebidas inicialmente para estos procesos, y con los avances tecnológicos existe una falta de regulación normativa (DiazGranados, 2016).

Para el manejo del *big data* es importante tener en cuenta que es muy diferente que en un país se encuentre una tecnología a que la misma sea realmente adoptada como propia. A eso se le denomina transferencia de tecnología, la cual es fundamental para el desarrollo de un conocimiento propio por parte de los países en desarrollo. Es por ello que, en el caso del software, en Colombia la legislación lo asimila a la escritura de una obra literaria, permitiendo que el código fuente de un programa esté cubierto por la Ley de derechos de autor (Propiedad intelectual en la legislación colombiana, s.f.)

De otra parte, elementos como la privacidad, los límites sobre la información personal, los derechos de autor y la confiabilidad son asuntos que deben tratarse antes de implementar estrategias de análisis masivo de información; en el proceso de compilar y tratar grandes cantidades de información para un tema específico, se pueden generar nuevos problemas, ya que dicha información puede ser usada potencialmente para abusar de la privacidad de las personas.

En este sentido, las leyes de protección de datos alrededor del mundo se han basado en los principios de notificación/conciencia y consentimiento/elección para permitir la utilización de datos, ya que el originario de estos debe conocer y entender que van a ser recolectados, así como saber para qué fin, y tras esto tiene que dar el consentimiento, y aceptar el cometido que se le dará a su información (DiazGranados, 2016).

De otro lado, la mayoría de beneficios del uso de *big data* en el sector público son similares a los del privado y están relacionados con una mejor toma de decisiones, óptima segmentación de poblaciones para focalizar acciones, innovación en modelos de negocio, eficiencia y efectividad; así como servicios de mayor calidad para los ciudadanos, al igual que reducción de amenazas de seguridad y crimen. Adicionalmente, *big data* ofrece oportunidades para mejorar en transparencia y participación ciudadanas (Fernández Gómez, 2014).

El uso de *big data* en el Gobierno puede facilitar la identificación de inconsistencias, errores y fraudes en impuestos, sistema de salud y programas de bienestar social. Con respecto a la seguridad, el uso de diferentes fuentes de datos podría ayudar a detectar e individualizar riesgos, motivos y organizaciones involucradas en terrorismo o ciberataques. Además de esto, esta implementación tecnológica podría contribuir en estudios forenses y protección de infraestructura crítica, aplicación de la ley y prevención de desastres (Fernández Gómez, 2014).

En Colombia, el Ministerio TIC reconoce el valor de la información como herramienta para el fortalecimiento de sectores industriales, gubernamentales y académicos. La existencia de información disponible hace de su consecuente análisis un insumo cada vez más valioso en la toma de decisiones; las tendencias mundiales en TIC evidencian la convergencia de tecnologías necesarias para el análisis de datos; es por esto que el *big data analytics* se posiciona

progresivamente en el centro de las estrategias sociales, económicas, culturales y políticas, y su eficacia significa la preparación de los recursos necesarios para su desarrollo.

En concordancia con tal lineamiento, el Ministerio TIC creó los Centros de Excelencia y Apropiación (en adelante: CEA) con el fin de aprovechar el *big data analytics* en sectores estratégicos. Con los CEA, la cartera en referencia busca la creación de valor a partir de *big data anlaytics* para ciberseguridad, internet de las cosas y la formulación de política pública (Min. Tic, s.f.).

En otros frentes del sector público, el país también ha avanzado con algunos proyectos piloto, entre estos se encuentra el realizado por el Departamento Administrativo Nacional de Estadística (en adelante: DANE), en el cual emplea *big data* para el monitoreo de los Objetivos de Desarrollo Sostenible y el Censo Nacional de Población y Vivienda. De igual manera, el Ministerio de Hacienda junto con el Departamento Nacional de Planeación (en adelante: DNP) han avanzado en una metodología, a partir de datos de Google Trends, que analiza la frecuencia de términos de búsqueda para inferir actividad económica en ciertos sectores y obtener indicadores que antes se adquirían con estadísticas tradicionales (ICDE, s.f.).

Otro avance significativo en el uso de estas tecnologías es la creación de "La Biblioteca Virtual en Salud para la Vigilancia en Salud Pública", impulsada por el Ministerio de Salud y Protección social; se trata de un repositorio digital institucional, que tiene las características de un archivo electrónico de producción científica de una institución, en el que se puede buscar y recuperar información para usarse en el ámbito nacional e internacional (Palacios, Delgado, León, Montaño, y Estupiñán, 2014).

En Colombia también se destaca la creación de alianzas entre el sector público y el privado para fortalecer la generación de soluciones en análisis de información. Un ejemplo de esto es la

Alianza Caoba o Centro de Excelencia y apropiación del *Big Data y Data Analytics*, cuyo objetivo es generar soluciones en diversos sectores industriales, gubernamentales y académicos.

Este centro de excelencia apoya el uso de las tecnologías de *big data* a través de diferentes frentes, incluye formación de talento humano, investigación aplicada y desarrollo de productos cuyo valor está fundado en este tipo de avances (Alianza Caoba, 2017).

Tras este recuento, es necesario resaltar que el uso estratégico del *big data* se fundamenta en la existencia de un marco de arquitectura empresarial que promueva estándares, buenas prácticas e interoperabilidad para todo el sector público:

Según Bohórquez, citado por Fernández Gómez (2014) "uno de los pilares de este marco, en términos de compras y contratación, es la preferencia por soluciones en la nube en vez de infraestructura propia" (p. 45), así —continúa Fernández Gómez— "[...] los acuerdos con el programa de Compra Eficiente, la infraestructura tecnológica para big data estaría disponible a través de servicios en la nube [...] bajo acuerdos de precios aplicables a todo el sector público y estandarización en tecnología, calidad y variedad de proveedores (Fernández Gómez, 2014, p. 45)".

En este contexto si lo que se busca es la aplicación de analítica en la investigación penal, debe señalarse que es necesario delimitar normativamente sus componentes, elementos, finalidades y límites propios.

4.2.1.2. Ciberseguridad y ciberdefensa en torno a la administración electrónica como estructura crítica del Estado y su relación con tendencias de análisis masivo de información.

Para hablar de ciberseguridad y ciberdefensa hay que referirse primero a ciberespacio. Este último es el espacio artificial creado por el conjunto de sistemas de la información y telecomunicaciones que utilizan las TIC, es decir de redes de ordenadores, mucho más que internet, más que los mismos sistemas y equipos, el hardware y el software e incluso que los propios usuarios, es un nuevo espacio, con sus propias leyes físicas que, a diferencia de los demás, ha sido creado por el hombre para su servicio (Min. Defensa España y IEEE, 2012).

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

Ahora bien, para entender qué es ciberseguridad, además del anterior concepto, se debe partir de conocer qué es seguridad de la información. Esta se define como la preservación de la confidencialidad, integridad y disponibilidad de la información, donde confidencialidad se entiende como una propiedad, a saber, que la información no sea puesta a disposición de otros sin autorización; integridad, por su parte, es la propiedad de mantener la exactitud y *completitud* de la información; y disponibilidad es la propiedad de que la información sea accesible y utilizable ante el requerimiento de una entidad autorizada (Kosutic, D., 2012).

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

En este orden de ideas, el crecimiento exponencial en el uso de internet, que se ha producido en todo el mundo, le ha dado mayor valor a la seguridad y esta le preocupa cada vez más a los habitantes de diferentes países. Es precisamente por esto, y para tratar de combatir las actividades ilegales que se desarrollan en la red, que al interior de la Unión Europea se ha empezado a legislar en torno a la ciberseguridad para su ciudadanía (Aucal Business School, 2016).

Una de las últimas actuaciones en este sentido fue el desarrollo de la Estrategia de Ciberseguridad Europea, nacida como un conjunto de acciones encaminadas a solventar y mejorar el espacio en la red. El documento nació arropado por una serie de órganos, instituciones y políticas que ya se habían estado trabajando alrededor de las diversas dimensiones de la seguridad desde finales de 1990 (Machín y Gazapo, 2016).

La estrategia de ciberseguridad de la Unión Europea establece los planes para prevenir y responder a las perturbaciones y ataques que pudieran afectar a los sistemas de telecomunicaciones de este bloque de países. La UE tiene, en este contexto, una extraordinaria importancia, no solo porque agrupa a 28 países industrializados —que en la economía digital mundial juegan un papel relevante— sino que en ellos las tecnologías digitales son el paradigma sobre la economía y la sociedad en su conjunto, mucho más que en otro lugar.

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

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

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

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

4.2.1.3. Seguridad Cibernética: OEA, el caso de la región.

La Organización de Estados Americanos (en adelante: OEA) ha estado trabajando para fortalecer las capacidades de seguridad cibernética entre sus Estados miembros desde principios de la década de 2000.

Con los años se ha convertido en un líder regional en asistencia a los países para fortalecer la capacidad técnica y de seguridad cibernética en cuanto a políticas para garantizar un ciberespacio seguro y resiliente. El programa de seguridad cibernética de la OEA apoya las iniciativas sobre la base de un análisis en profundidad y la comprensión de la magnitud de las amenazas (OEA, 2015).

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

Los Estados miembros fueron extraordinariamente previsivos cuando adoptaron tal estrategia, ya que se ha mejorado la protección de la infraestructura de las TIC con el fortalecimiento de la capacidad de los gobiernos para responder y mitigar incidentes cibernéticos. Estos compromisos se han reafirmado y fortalecido con los años a partir de la adopción de numerosas declaraciones oficiales, incluyendo la más reciente relacionada con el papel y las responsabilidades de la OEA y sus Estados miembros en la promoción de la seguridad cibernética, la lucha contra la delincuencia informática y la protección de infraestructuras de información crítica (OAS, 2016).

4.3.1.4. La política nacional de seguridad digital colombiana – elementos críticos.

4.3.1.4.1. Estructura y desarrollo de la política nacional de seguridad digital.

El documento Conpes 3854 de seguridad digital parte de un diagnóstico del que se podría resaltar la determinación de ausencia de una visión estratégica basada en la gestión de riesgos; así mismo, las múltiples partes interesadas no maximizan sus oportunidades al desarrollar actividades socioeconómicas en el entorno digital (Conpes, 2016).

Además, se establece que es necesario reforzar las capacidades de ciberseguridad con un enfoque de gestión de riesgos, así como reforzar las de ciberdefensa con un enfoque de gestión de riesgos; también se determina que los esfuerzos de cooperación, colaboración y asistencia, nacionales e internacionales, relacionados con la seguridad digital, son insuficientes y desarticulados. Ante este panorama se plantea una nueva política, cuyo objetivo general es:

> [...] identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país. (Conpes, 2016, p 47)

Dicho objetivo general se desarrollará a través de cinco estrategias tendientes a:

> i) Establecer un marco institucional para la seguridad digital consistente con un enfoque de gestión de riesgos [...] ii) 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 [...] iii) Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos [...] iv) Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos [...] v) Generar mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad digital, a nivel nacional e internacional. (Conpes, 2016, p 48-49)

4.3.1.4.2. Establecer un marco institucional para la seguridad digital consistente con un enfoque de gestión de riesgos.

Entre los elementos destacables del documento Conpes en comento está la creación de la figura de coordinador nacional de seguridad digital, el cual tendrá entre sus funciones:

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

De igual modo este coordinador debe propender por:

> Garantizar que los programas, proyectos y campañas de concientización y sensibilización, así como las capacitaciones que adelanten las diferentes entidades, se diseñen a partir de

> los lineamientos y orientaciones que emita la Comisión Nacional Digital y de Información Estatal, o de quien haga sus veces, con el fin de evitar la duplicación de esfuerzos y garantizar la eficiencia en el manejo de los recursos; recomendar nuevas acciones en colaboración con las múltiples partes interesadas, en vista de la rápida tasa de desarrollo de la tecnología y los escenarios de ataques cibernéticos; coordinar con la comisión Nacional Digital y de Información Estatal, y con las múltiples partes interesadas, los informes respecto del cumplimiento de los lineamientos de orientación superior establecidos para la implementación de la política nacional de seguridad digital en el marco de sus principios fundamentales. (Conpes, 2016, p 50)

4.3.1.4.3. Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital.

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

4.3.1.4.4. Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos.

Es necesario empoderar a los ciudadanos y al Estado en relación con los riesgos del entorno digital, y consolidar las capacidades del país para hacer frente al crimen, la delincuencia y otros fenómenos que afectan la seguridad nacional en este espacio. Para esto es imperativo fortalecer a las entidades responsables de ciberseguridad; adecuar el marco jurídico referente a los cibercrímenes y ciberdelincuencia, así como socializar y concientizar acerca de estos a las múltiples partes interesadas; también hay que fortalecer las capacidades de los responsables de seguridad nacional en el ciberespacio y la de judicialización de este tipo de conductas.

4.3.1.4.5. Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos.

Es fundamental desarrollar capacidades de prevención, detección, contención, respuesta, recuperación y defensa para garantizar los fines del Estado, así como mejorar la protección, preservar la integridad y la resiliencia de la infraestructura crítica cibernética nacional; para lo cual es necesario fortalecer las instancias y entidades responsables de la defensa nacional en el entorno digital, adecuar el marco jurídico para abordar la protección y defensa del mismo; generar una estrategia de protección y defensa de la infraestructura crítica cibernética nacional, fortalecer el esquema de identificación, prevención y gestión de incidentes digitales, con la

participación activa de las múltiples partes interesadas, y fortalecer las capacidades de los responsables de garantizar la defensa nacional en el entorno digital.

4.3.1.4.6. Generar mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad digital, a nivel nacional e internacional.

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

4.3.1.4.7. Elementos críticos del documento - necesidades de desarrollo.

Me limitaré exclusivamente a enunciar los elementos críticos para desarrollar, y que se convierten en el verdadero reto para la efectividad de esta nueva política se seguridad electrónica.

Hablamos así de: i) la elaboración y ejecución de los planes de fortalecimiento de las capacidades operativas, administrativas, humanas, científicas, ii) la elaboración y ejecución del plan de fortalecimiento de las capacidades institucionales, operativas, administrativas, humanas, de infraestructura física y tecnológica del sector inteligencia, iii) el diseño de un modelo de gestión de riesgos de seguridad digital a nivel nacional, iv) el ajuste al marco regulatorio del sector de Tecnologías de la Información y las Comunicaciones, teniendo en cuenta aspectos necesarios para la gestión de riesgos de seguridad digital, v) la creación de una agenda estratégica nacional e internacional en temas de seguridad digital, vi) la adaptación e implementación de un modelo de gestión de riesgos de seguridad digital a nivel nacional (Min TIC, 2015).

4.3.1.4.8. Ciberdefensa.

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

Ciberdefensa es, entonces, el conjunto de acciones u operaciones activas o pasivas desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal de los recursos informáticos y teleinformáticos de la defensa a fin de asegurar el cumplimiento de las misiones o servicios para los que fueran concebidos, a la vez que se impide que fuerzas enemigas los utilicen para cumplir los suyos.

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

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

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

En este punto es importante reseñar que en el país se cuenta con el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (en adelante: Colcert), el cual tiene como responsabilidad central la coordinación nacional de la ciberseguridad y ciberdefensa, la cual estará enmarcada dentro del proceso misional de gestión de la seguridad y defensa del Ministerio de Defensa Nacional.

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

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

No obstante, no es claro si esto se debió a una reducción real en el número de incidentes o a una mejor gestión de la seguridad por parte de las agencias gubernamentales atendidas por estos equipos nacionales de respuesta a incidentes de seguridad cibernética, como son los CSIRT, o a la

implementación de políticas que cambiaron la cobertura de la asistencia prestada por los equipos de respuesta de Colombia (OEA, 2013).

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

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

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

5. Estrategia de ciberseguridad para la Fiscalía General de la Nación como elemento integrador de la estrategia de utilización de tecnologías de la información y las comunicaciones

5.1. De la ciberseguridad

5.1.1. Para iniciar tenemos.

La Guía de Ciberseguridad para los Países en Desarrollo de 2007 se presenta como uno de los documentos necesarios para entender la importancia de establecer estrategias de ciberseguridad en el marco del cumplimiento de los objetivos y la misión de las organizaciones públicas y privadas en Latinoamérica. Como lo he señalado a lo largo de este trabajo, la utilización de TIC para el cumplimiento de objetivos organizacionales trae aparejados riesgos; lo que lleva a la necesidad de diseñar planes de desarrollo de infraestructuras y servicios digitales que comprendan una estrategia multidisciplinar de la ciberseguridad coherente, eficaz y controlable, que se dirija a cumplir un fin claro; el cual, en palabras de la Unión Internacional de Telecomunicaciones (en adelante: UIT), se puede definir así:

> El objetivo de la ciberseguridad es contribuir a la preservación de las fuerzas y medios organizativos, humanos, financieros, tecnológicos e informativos, adquiridos por las instituciones, para realizar sus objetivos. La finalidad de la seguridad informática es conseguir que ningún perjuicio pueda poner en peligro su perpetuidad. Para ello se tratará de reducir la probabilidad de materialización de las amenazas; limitando los daños o averías resultantes; y logrando que se reanuden las operaciones normales tras un incidente de seguridad, en un plazo de tiempo razonable y a un coste aceptable. (UIT, 2007, p. 5)

Plantear una estrategia de ciberseguridad implica la identificación de los activos, los recursos a proteger, los actores implicados, la determinación de un conjunto de normas éticas y jurídicas; así como un conjunto de lineamientos, la determinación de los planes de formación al personal, la incorporación de un esquema integral de implementación de tecnologías; al igual que actividades preventivas, de gestión de los riegos, reactivas y, por supuesto, colaboración y cooperación; ya que se debe entender que no podemos actuar solos.

La ciberseguridad se debe entender desde una visión integral, pero sobre todo desde la responsabilidad, y esto implica reducir la brecha digital; para lo cual, según la UIT, se exigirán, entre otros, infraestructuras de información fiables y seguras, políticas que propicien confianza, un marco jurídico adecuado; así como autoridades políticas y jurídicas versadas en las nuevas tecnologías y, sobre todo, gestión del riesgo y seguridad de la información, siempre teniendo de presente el respeto y garantía de los derechos humanos, especialmente cuando se trata de protección de datos personales.

5.1.2. Concepto de ciberseguridad.

La Asociación de Auditoría y Control sobre los Sistemas de Información —*Information Systems Audit and Control Association* (en adelante: Isaca)— define la ciberseguridad como "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados" (Audea.com, 2016, párr. 3).

En este orden de ideas, la protección de la confidencialidad, integridad y la disponibilidad de la información, la capacidad de prevención, la seguridad de los sistemas, la capacidad de investigación y persecución, la resiliencia y la cultura de ciberseguridad se convierten en el eje transversal de análisis y desarrollo de cualquier estrategia de ciberseguridad.

La ciberseguridad tiene como foco la protección de la información digital de los sistemas interconectados; por consiguiente, es un área que se encuentra comprendida dentro de la seguridad informática o seguridad digital, que involucra métodos, procesos y técnicas para el tratamiento de la información en formato digital, pero no solo eso sino la protección de redes e infraestructuras.

5.2. La necesidad de una estrategia de utilización de medios electrónicos en la Fiscalía General de la Nación como inicio para el diseño de una estrategia de ciberseguridad.

5.2.1. Plan estratégico de gobierno electrónico para la Fiscalía General de la Nación.

Este trabajo le da continuidad al proceso académico cursado en la Universidad de Valencia, España, a partir del cual surgió mi tesis doctoral "El derecho a la buena Administración electrónica" (2015), dado que en su tema principal se circunscribe la e-justicia; la cual, a su vez, es uno de los principales aspectos en este documento, del que se infiere que para que esta exista de verdad se deben aplicar aspectos propios de las TIC como el *big data* y la ciberseguridad, que también hagan viable la estrategia de gobierno electrónico que aquí se propone para la FGN.

Por lo anterior, me permito guiar el desarrollo de este Plan estratégico a partir de las propuestas presentadas en diversos apartados de la tesis aludida, principalmente en los intitulados "La buena eAdministración en Colombia" (p. 82), "El debido proceso en el ámbito de la

Administración pública electrónica" (p. 153), así como en los denominados, "¿Buena eAdministración o gobierno abierto?" (p. 90) y "Gobernanza y buena Administración" (p. 19).

5.2.2. ¿Con el marco jurídico existente se puede establecer una estrategia de e-gobierno en la FGN?

Los avances propios de la sociedad de la información, ya descrita en la presente tesis, han dado lugar a que la Administración pública genere canales de comunicación con los ciudadanos a través de medios electrónicos. Lo propio ha sucedido con la Administración colombiana, que ha visto en las TIC un medio eficaz para alcanzar sus fines (Sánchez Acevedo, 2015).

Como lo menciono en la tesis de doctorado, a consecuencia de la anterior circunstancia, Colombia tuvo que incluir, dentro de su marco jurídico, normas relativas al uso de las TIC en las relaciones con sus administrados.

Para contestar la pregunta que encabeza esta sección, procedo a presentar una relación cronológica de leyes, sobre el tema en cuestión, al igual que de actos administrativos y políticas diseñadas por el Ejecutivo, que en su momento también fueron reseñados más ampliamente en la tesis doctoral (pp. 82 - 90). Veamos:

Decreto 2150 de 1995: marcó la pauta en el uso de herramientas electrónicas como un medio para simplificar algunos trámites ante las entidades; estableció que estas debían habilitar sistemas de transmisión electrónica en cuanto a sus actuaciones con la Administración.

Documento Conpes de 1995: aprobado por el Departamento Nacional de Planeación (en adelante: DNP) y emitido a consecuencia del anterior decreto; contiene una estrategia orientada al

uso de los recursos públicos que contempla la creación de la Unidad de Eficiencia de la Consejería Presidencial para el Desarrollo Institucional, el desarrollo de las facultades extraordinarias de la Ley 190 de 1995, así como el sistema de información normativa y de procesos de la Administración Pública.

Decreto 1122 de 1999: representó un avance porque autorizaba a la Administración Pública y a los particulares que ejercían funciones administrativas a usar cualquier medio tecnológico o documento electrónico, con condiciones y requisitos de seguridad; sin embargo, fue declarado inexequible por la Corte Constitucional, en su sentencia C-923 de 1999, por los vicios de forma.

Es destacable el hecho de que este decreto permitía presentar peticiones, quejas o reclamos ante cualquier autoridad a través de mensajes de datos, así como facilitar el acceso a información de la entidad mediante internet.

Ley 527 de 1999: define y reglamenta el acceso y el uso de los mensajes de datos, comercio electrónico y firmas digitales. "[...] no intentó reencaminar la Administración Pública convencional a través de medios electrónicos, sí abrió paso para que se utilizaran los medios electrónicos como un "puente" entre comerciantes para realizar sus transacciones a través de estos instrumentos" (Sánchez Acevedo, 2015, p. 83).

Documento Conpes 3072: documento del 9 de febrero de 2000, emitido por el Consejo Nacional de Política Económica y Social (en adelante: Conpes), y el Ministerio de Comunicaciones, hoy Min TIC. Estableció y aprobó la Agenda de Conectividad; esta buscó la expansión de las TIC, la competitividad del sector productivo y la modernización de las instituciones públicas y el Gobierno, al igual que socializar el acceso a la información.

Gobierno en Línea: estrategia del año 2000 creada por la Presidencia de la República que se reflejó especialmente en el portal www.gobiernoenlinea.gov.co, según la Directiva Presidencial No. 2. de ese año su finalidad era la de:

> [...] proveer al Estado de una conectividad que facilite la gestión en línea de los organismos gubernamentales y apoye su función de servicio al ciudadano, como un complemento al esquema actual, en el que se realizan estos procesos en forma presencial en las oficinas del Gobierno y se sustentan con documentos escritos en papel [...] (p. 2)

Directiva Presidencial No. 10 del 20 de agosto de 2002: se dio bajo el mandato de Álvaro Uribe Vélez, estatuyó el Programa de Renovación de la Administración Pública, que ordena que cada entidad dentro de la organización, y según su capacidad, debe crear un sistema que garantice que los ciudadanos puedan acceder en todo momento a la información pública.

Ley 790 de 2002: incluye disposiciones para implementar el programa de renovación de la Administración Pública para la atención de la ciudadanía, en concordancia con los principios de la inmediación y la celeridad. Además, prescribió que el Gobierno Nacional promovería el desarrollo de tecnologías y procedimientos del e Gobierno o en línea.

Documento Conpes 3248 sobre la renovación de la Administración Pública: aprobado por el DNP el 20 de octubre de 2003, contenía reformas verticales y transversales dirigidas a la incorporación y el uso de la tecnología informática en el desarrollo de las actividades estatales, tanto al interior de las entidades como en aquellas que se dan con otras entidades públicas y privadas, así como con los ciudadanos y el sector productivo.

Ley 962 de 2005: dicta disposiciones sobre la racionalización de trámites y procedimientos administrativos de los organismos y las entidades del Estado y de los particulares que ejercen

funciones públicas o prestan servicios públicos. Uno de sus principios es el fortalecimiento económico de la actuación de la Administración Pública, al igual que la disminución de los tiempos y los costos de trámites por parte de los administrados, a través de los medios tecnológicos integrados.

Es relevante lo que expresa su artículo 6, dedicado a los medios tecnológicos, pues autoriza el uso de soportes, medios y aplicaciones electrónicas para el trámite, la notificación y la publicación de actos administrativos; asimismo, se indica que los ciudadanos podrán presentar peticiones, quejas, reclamaciones o recursos a través de un medio tecnológico o electrónico del que dispongan las entidades y los organismos de la Administración Pública.

Acuerdo No. PSAA06-3334 de 2006 del Consejo Superior de la Judicatura (Sala Administrativa): reglamentó el uso de medios electrónicos e informáticos en el cumplimiento de las funciones de la Administración de justicia.

Ley 1147 de 2007: creó la Comisión Especial de Modernización y las Unidades Coordinadoras de Asistencia Técnica Legislativa y Atención Ciudadana del Congreso de la República. La Comisión Especial de Modernización, entre sus funciones, debía establecer los términos y los procedimientos para actualizar la información contenida en la página de Internet del Congreso de la República.

Ley 1341 de 2009: definió los principios y los conceptos sobre la organización de las TIC, y creó la Agencia Nacional de Espectro. Determinó como prioritarios el acceso y el uso de las TIC respecto a la producción de bienes y servicios, en condiciones no discriminatorias de conectividad, educación y competitividad.

Decreto 2623 del 13 de julio de 2009: "[...] creó el Sistema Nacional de Servicio al Ciudadano como una instancia "coordinadora para la Administración Pública Nacional de las

políticas, estrategias, programas, metodologías, mecanismos y actividades encaminadas a fortalecer la Administración al servicio del ciudadano [...]" (p. 2).

Ley 1437 de 2011, por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo: el CPACA tomó como uno de sus principios base el incentivo al uso de las TIC, para efectos de que los procedimientos se adelantasen con diligencia, dentro de los términos legales y sin dilaciones injustificadas (Sánchez Acevedo, 2015, p. 89).

En la tesis doctoral también manifesté que esta ley "declaró la validez de los documentos públicos en medios electrónicos y la notificación electrónica, así como el expediente electrónico, la sede electrónica y los procedimientos para recibir documentos electrónicos" (p. 89). Asimismo, este Código también estipuló "la presentación de peticiones por cualquier medio tecnológico o electrónico disponible en una entidad de la Administración, así como la generación de procedimientos mediante las TIC, y comunicar a terceros las actuaciones administrativas por correo electrónico" (p. 89)

El CPACA contiene normas que propician la prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública. Su artículo 74 señala que todas las entidades del Estado deberán publicar en su sitio web el plan de acción para el año siguiente, al igual que el presupuesto debidamente desagregado.

Directiva Presidencial 04 del 3 de abril de 2012: emitida por el presidente de la República, Juan Manuel Santos Calderón; está dedicada a señalar políticas sobre eficiencia administrativa y especialmente en cuanto a la Política Cero Papel en la Administración Pública, esta implica el cambio del material documental o físico por soportes y medios electrónicos.

Otras normas que contienen avance en cuanto al uso de medios electrónicos son la Ley 1564 de 2012, por la se expide el Código General del Proceso.

Ley Estatutaria 1581 de 2012 o Estatuto de protección de datos personales: Por la cual se dictan disposiciones generales para la protección de datos personales y de acuerdo con su objeto, establecido en el artículo primero tiene el fin de "desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma"

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, según su epígrafe, y de acuerdo con su artículo 1° "tiene el objeto de regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información".

Ley 1755 de 2015: regula el derecho fundamental de petición, al igual que sustituye los artículos 13 a 33 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, que habían sido declarados inconstitucionales puesto que este derecho se debe desarrollar a través de una ley estatutaria.

Es precisamente aquí donde aparece la primera gran conclusión y está relacionada con que el conjunto normativo colombiano no contiene normas propias para la Fiscalía General de la Nación que tengan como finalidad la implementación de una estrategia de gobierno digital para el cumplimiento de su función misional, establecida en el artículo 250 de la Constitución.

En consecuencia, no hay un soporte jurídico suficiente que permita la incorporación de TIC en la Administración de justicia y, de manera específica, en la Fiscalía, en los términos del parágrafo 1 del artículo 2 del decreto 2573 de 2014 el cual establece que "La implementación de la estrategia de Gobierno en línea en las Ramas legislativo y Judicial, en los órganos de control, en los autónomos e independientes y demás organismos del Estado, se realizará bajo un esquema coordinación y colaboración armónica en aplicación los principios señalados en artículo 209 de la Constitución Política".

5.2.3. Los elementos de una estrategia de gobierno digital para la Fiscalía General de la Nación.

5.2.3.1. El debido proceso electrónico y el cumplimiento del principio de legalidad como elemento fundamental de la estrategia de gobierno digital de la Fiscalía.

El derecho al debido proceso, y en especial al debido proceso electrónico, es un elemento de la e-administración, ya que esta se fundamenta en el respeto a tal derecho. Asimismo, este se encuentra ligado al derecho al debido proceso administrativo y al de una buena Administración (Gamero Casado, 2008) y, por ende, a una buena Administración de justicia, así como a la posibilidad de la e-justicia.

Sobre el derecho al debido proceso, y su vinculación con el debido proceso administrativo, la jurisprudencia colombiana ha abundado; para la muestra, la Corte Constitucional, expresó sobre este derecho de rango fundamental que: "es un derecho constitucional fundamental, consagrado

expresamente en el artículo 29 de la Constitución Política, el cual lo hace extensivo 'a toda clase de actuaciones judiciales y administrativas'" (CConst., 2010, C-980, p. 17).

Del mismo modo, este alto tribunal también se ha pronunciado sobre el derecho al debido proceso administrativo, como tal, al referirse a las garantías mínimas previas y posteriores en la sentencia de constitucionalidad con radicado C-034 (2014):

> Las garantías mínimas previas se relacionan con aquellas (que) [...] deben cobijar la expedición y ejecución de cualquier acto o procedimiento administrativo [...] de otro lado, las garantías mínimas posteriores se refieren a la posibilidad de cuestionar la validez jurídica de una decisión administrativa, mediante los recursos de la vía gubernativa y la jurisdicción contenciosa administrativa. (P. 1)

Es necesario decir que el debido proceso administrativo encuentra su fundamento no solo en el artículo 29 de la Constitución, sino en el 209 de la misma normativa superior, referente a la función administrativa y de ahí radica que "el debido proceso administrativo deba armonizar los mandatos del artículo 29 Superior con los principios del artículo 209, ibídem." (C.Cons, 2014, C-034, p. 20).

Ahora bien, la Administración de justicia —de la que se tiene que derivar la e-justicia— está consagrada como función pública en el artículo 228 superior; así mismo, el artículo 229 constitucional "garantiza el derecho de toda persona para acceder a la Administración de justicia", (Constitución Política; en adelante CN, 1991), y la Ley Estatutaria de Administración de Justicia, Ley 270 de 1996, también consagra este último derecho en su artículo 2, según lo ha explicado la Corte Constitucional en su sentencia de tutela con radicado T-283 de 2013.

El máximo tribunal de lo constitucional se ha pronunciado sobre el contenido del derecho a la Administración de justicia en los siguientes términos:

> El derecho a la Administración de justicia ha sido definido por la jurisprudencia constitucional como la posibilidad reconocida a todas las personas residentes en Colombia de poder acudir en condiciones de igualdad ante los jueces y tribunales de justicia, para propugnar por la integridad del orden jurídico y por la debida protección o el restablecimiento de sus derechos e intereses legítimos, con estricta sujeción a los procedimientos previamente establecidos y con plena observancia de las garantías sustanciales y procedimentales previstas en las leyes. (C.Cons, 2013, T-283, p. 26)

Igualmente, la Corte Constitucional ha hecho enlistado los derechos que integran el debido proceso administrativo de la siguiente manera:

> "[…] hacen parte de las garantías del debido proceso administrativo, entre otros, los derechos a: (i) ser oído durante toda la actuación, (ii) a la notificación oportuna y de conformidad con la ley, (iii) a que la actuación se surta sin dilaciones injustificadas, (iv) a que se permita la participación en la actuación desde su inicio hasta su culminación, (v) a que la actuación se adelante por autoridad competente y con el pleno respeto de las formas propias previstas en el ordenamiento jurídico, (vi) a gozar de la presunción de inocencia, (vii) al ejercicio del derecho de defensa y contradicción, (viii) a solicitar, aportar y controvertir pruebas, y (ix) a impugnar las decisiones y a promover la nulidad de aquellas obtenidas con violación del debido proceso" . (C.Cons 2013, C-758, p. 25), citada por Sánchez Acevedo 2015, p. 153)

En concordancia con lo expuesto, del debido proceso se desprende el procedimiento penal, al cual le es predicable lo referido en mi tesis doctoral acerca del procedimiento administrativo, pues sobre este, en su momento mencioné que:

> [..] se fundamenta en uno de los elementos estructurales del Estado de Derecho: el principio de legalidad, entendido este como la sujeción de los poderes públicos al ordenamiento jurídico, lo cual es consecuencia, a su vez, del conjunto de reglas que rigen la actuación de las autoridades [...] La existencia de formas predeterminadas en la ley limita la improvisación y preserva la jerarquía de las organizaciones administrativas. Adicionalmente, racionaliza su funcionamiento, pues ordena la actividad y reduce o evita ineficiencias. Además, torna previsible para los terceros el comportamiento de las autoridades y los resultados de este [...] E. Díaz (2002), citado por Sánchez Acevedo (2005, pp. 148-149)

A lo mencionado se suma, que el derecho al debido proceso contiene otras prerrogativas como el derecho de toda persona a ser oída antes de que en su contra se tome una medida que le desfavorezca y el derecho de acceder al expediente que le concierna dentro del respeto de los intereses legítimos de la confidencialidad y del secreto profesional y comercial, por ejemplo, esta garantía se constata en el Sistema Penal Acusatorio (Ley 906 de 2004) desde el momento en que una noticia criminal aún está en la etapa de investigación, es decir, cuando todavía ni siquiera se ha hecho la vinculación formal del posible indiciado a través de la imputación.

El derecho en mención le impone a la Administración el deber de motivar sus decisiones, y a la parte interesada le otorga la facultad de aportar pruebas, recibir notificaciones de manera debida —bajo el principio de publicidad— impugnar las decisiones, entre otros estipulados en el

artículo 29 constitucional, y en el 31 del mismo rango, inclusive, que le da continuidad al mencionado derecho de controvertir las decisiones y lo adiciona en el sentido de que "el superior no podrá agravar la pena impuesta cuando el condenado sea apelante único" (Col, CN, art 31).

De lo anterior se infiere que toda Administración requiere el respeto al debido proceso, pues este permite abordar las necesidades inherentes a sus procesos internos, así como aquellas que se dan en relación con la ciudadanía.

Es claro entonces que para que un procedimiento administrativo o judicial responda al principio de legalidad, o al debido proceso, debe estar previamente estipulado dentro del ordenamiento jurídico, y en dicho procedimiento deben encontrarse una serie de garantías mínimas a favor de los administrados, que les determinen un derrotero cierto para acudir a la jurisdicción o a entenderse con aquellos que ejercen la función pública.

Haciendo referencia a Esparza Leibar (1995), el debido proceso viene siendo un derecho correlativo, teniendo en cuenta que en los términos de esta autora hay una cadena de derechos y obligaciones que corresponden a cada una de las partes en la relación Administración-administrado, y si se tiene claro qué debe acontecer en esas cadenas, ante determinados fallos o eventualidades, tanto una parte como la otra pueden determinar qué sucedió y así verificar si se vulneró o no un derecho.

Un clásico ejemplo de lo anterior lo podemos encontrar en la caducidad que se puede generar como castigo al administrado por no haber ejercido un derecho en los tiempos que señala la ley; pero ante esto se puede presentar el caso de que la omisión del afectado se haya dado porque se hubiese presentado una indebida notificación de la decisión judicial o del acto administrativo;

entonces, en este caso, quien no siguió la cadena de obligaciones y por ende afectó la cadena de derechos fue la entidad pública.

De acuerdo con lo anterior, el primero de los elementos de una estrategia de gobierno digital es el respeto por el debido proceso penal y las garantías que de él se derivan, ya señaladas anteriormente; de las cuales podríamos resaltar aquellas cuya trascendencia, por el uso de medios electrónicos, deben ser estudiadas. Entre estas se encuentran: la igualdad como garantía del debido proceso electrónico, la aportación de pruebas por medios electrónicos, la publicidad como garantía del debido proceso electrónico y la neutralidad tecnológica.

5.2.3.2. Diseño de una arquitectura institucional para la Fiscalía General de la Nación.

Si seguimos la estructura planteada por el Decreto de Gobierno Digital 2573 de 2014, los fundamentos de la Estrategia para la Fiscalía General de la Nación deben ser desarrollados a través de 4 componentes:

5.2.3.2.1. TIC para servicios.

En los términos del Decreto 2573 de 2014 esta fase comprende "la provisión de trámites y servicios a través de medios electrónicos, enfocados a dar solución a las principales necesidades y demandas de los ciudadanos y empresas, en condiciones de calidad, facilidad de uso y mejoramiento continuo".

5.2.3.2.2. TIC para el gobierno abierto.

En la tesis de la Universidad de Valencia (2015), manifesté, a propósito de la e-administración, que la instauración de ciertos mecanismos, destinados a la transparencia de los gobiernos, propician ámbitos de colaboración y participación que superan con creces el simple sufragio y que dichos mecanismos sustentan un estado de la evolución de los sistemas democráticos que han redundado en el nuevo paradigma del gobierno abierto; cuyo concepto presenté, valiéndome de los aportes de Llinares (s.f.) de la siguiente manera:

> [...] Un gobierno abierto es el que entabla una constante conversación con los ciudadanos, con el fin de escuchar lo que ellos dicen y solicitan; que toma decisiones basadas en sus necesidades y teniendo en cuenta sus preferencias; que facilita la colaboración de los ciudadanos y de los funcionarios en el desarrollo de los servicios que presta, y que comunica todo cuanto decide y hace, de forma abierta y transparente. (Sánchez Acevedo, 2015, pp. 90-91).

En mi tesis también referí que el primer manifiesto emitido desde la Casa Blanca, bajo la Administración de Barack Obama el *Open Government Memorandum* (Memorando de Gobierno Abierto), contiene los tres principios fundamentales del concepto de gobierno abierto, lo cuales son "transparencia, colaboración y participación".

Dicho memorando se menciona en el informe de la Comisión Económica para América Latina y el Caribe (en adelante: CEPAL) "El Desafío hacia el Gobierno Abierto" (CEPAL, 2012), el cual es categórico en señalar que hay que tener clara la diferencia entre *e-gobierno* (también llamado e-administración) y *gobierno abierto*.

Por ello, es importante advertir que el documento de la CEPAL recalca que el e-gobierno se refiere a la aplicación de las TIC a los procedimientos administrativos ya establecidos; aclara que este tipo de implementaciones, en sí mismas, no transforman a la sociedad, pero sí manifiesta que facilitan las relaciones de los ciudadanos y habitantes, en general, con las instancias del Estado, lo cual es muy valioso en términos de calidad de vida.

Gobierno abierto, por otro lado, es un concepto relativo a la filosofía del Gobierno, (CEPAL, 2012); involucra los dogmas y valores que demarcan su derrotero, los cuales se reflejan en una especie de rediseño en las Administraciones y Gobiernos.

Entonces, según el organismo de la ONU, al adoptar una política de gobierno abierto se deben dejar a un lado los trámites administrativos innecesarios, y abandonar el concepto dictatorial de administrado por el de ciudadano.

Por lo anterior, se entiende que cualquier proceso de gobierno abierto debe estar en concordancia con el proyecto de Estado que cada país tenga, el cual debe estar inserto en la carta constitucional correspondiente.

5.2.3.2.2. TIC para la gestión.

De acuerdo con el Decreto 2573 de 2014 esta fase incluye "[...] planeación y gestión tecnológica, la mejora de procesos internos y el intercambio de información. [...], la gestión y aprovechamiento de la información para el análisis, toma de decisiones y el mejoramiento [...] para una respuesta articulada del Gobierno y hacer más eficaz la gestión [...]".

5.2.3.2.3. Seguridad y privacidad de la Información.

Según el Decreto 2573 de 2014, esta fase se refiere a "acciones transversales a demás componentes enunciados, a proteger la información y sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada".

Precisamente, sobre este aspecto realizaré el análisis en cuanto a la necesidad de una estrategia para la FGN.

5.2.4. La necesidad de regular la estructuración del gobierno digital de la Fiscalía General de la Nación.

En el Plan Sectorial de Desarrollo Rama Judicial 2015 – 2018 se estableció como propósito esencial el mejoramiento de la gestión judicial y administrativa con fundamento en:

> [...] unas políticas institucionales que conlleven a la satisfacción de la demanda de justicia, mejoren los canales de interacción con el ciudadano, incorporando herramientas innovadoras que contribuyan a la celeridad y la simplificación del quehacer de la Administración de justicia. (2015, p. 101)

En el numeral 2 de dicho plan se elabora un diagnóstico de la Administración de justicia; en el tercero y siguientes se establece la política tecnológica, de la infraestructura, del talento, de la organización, de la democratización, de la calidad, entre otros. Allí se presenta la situación actual de la Administración de justicia y se señala que:

> [...] Para lograr el cometido fijado a la Administración de justicia como parte de la función pública de hacer efectivos los derechos, obligaciones, garantías y libertades, con el propósito de realizar la convivencia social [...] se ha instituido en la estructura de la Rama Judicial: (i)los órganos que integran las Jurisdicciones Ordinaria, de lo Contencioso Administrativo, Constitucional y de Paz; (ii) la Fiscalía General de la Nación y (iii) el Consejo Superior de la Judicatura (CSJud, 2015, p. 101).

Por tanto, se determina la estructura que cobija dicho plan y señala claramente que del mismo se excluye a la Fiscalía General de la Nación: "[…] asegura, la no inserción de la Fiscalía General de la Nación por su autonomía administrativa y presupuestal" (CSJud, 2015, p. 101).

Así las cosas, a pesar de que el artículo 209 constitucional establece, como principios del actuar de la Administración, la colaboración armónica, el Plan de la Administración de Justicia, vigente hasta 2018, no incorpora uno de sus órganos estructurales: La Fiscalía General de la Nación. Por ello, la segunda gran conclusión es la necesidad de regular la estructuración, desarrollo, incorporación, seguimiento y control del gobierno electrónico o digital en la FGN.

5.2.5. La necesidad de regular e implementar la identificación electrónica de servidores públicos y ciudadanos.

5.2.5.1. La necesidad de regular y proteger la infraestructura de la FGN.

La creciente utilización de tecnologías por las administraciones públicas trae consigo la necesidad de determinar si la infraestructura de tecnologías y la información, propiamente dicha, en que se funda la e-administración, tiene una categoría especial por proteger.

Desde ya se debe decir que no existe una norma colombiana que establezca que el daño a la infraestructura tecnológica de la Administración pública sea considerada de alto nivel y, por ende, que sea fundamental su protección.

Para brindar un ejemplo, en la Comunidad Europea se estableció en la Directiva de Ciberseguridad de 2016 la necesidad de determinar un conjunto de sectores necesarios para proteger y por tanto se le da la clasificación de infraestructura crítica, siendo necesaria una protección superior para garantizar unos mínimos que permitan el funcionamiento de dichos sectores (PE y Consejo de la UE, 2016). En esta directiva se evidencia la necesidad de dar unos parámetros para lo que se debe considerar un efecto perturbador significativo; para ello, se deben tener en cuenta al menos los siguientes factores intersectoriales:

> a) el número de usuarios que confían en los servicios prestados por la entidad de que se trate; b) la dependencia de otros sectores que figuran en el anexo II sobre el servicio prestado por esa entidad; c) la repercusión que podrían tener los incidentes, en términos de grado y duración, en las actividades económicas y sociales o en la seguridad pública; d) la cuota de mercado de la entidad; e) la extensión geográfica con respecto a la zona que podría verse afectada por un incidente; f) la importancia de la entidad para mantener un nivel suficiente del servicio, teniendo en cuenta la disponibilidad de alternativas para la prestación de ese servicio. (PE y Consejo de la UE, 2016, p. 15)

Entonces, debe entenderse la infraestructura crítica como aquella estratégica, cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales (España, Ley 8 de 2011).

Así las cosas, las instalaciones, equipos físicos y de tecnología de la información, redes, servicios y activos cuya interrupción o destrucción pueden tener grandes repercusiones en la salud, la seguridad o el bienestar económico de los ciudadanos o en el funcionamiento de los gobiernos de los Estados, deben protegerse (Comisión Europea, 2007b.), y para ello la utilización de técnicas de análisis masivo de información como el *big data* resultan fundamentales.

La puesta en marcha del Programa Europeo de Protección de Infraestructuras Críticas (en adelante: PEPIC), que tiene el objetivo de promover la creación de listas de infraestructuras críticas por parte de los Estados miembros en su territorio —así como preparar los análisis de vulnerabilidad y evaluación del riesgo, presentar soluciones y medidas de protección y fomentar la colaboración entre las empresas y las administraciones públicas en la protección de infraestructuras— resulta ser un claro ejemplo del camino por donde se debe ir la Fiscalía General de la Nación.

5.2.5.2. La necesidad de regular e implementar el expediente judicial electrónico.

Desde la Carta Magna promulgada por Juan sin Tierra en 1215, el *due process of law* (debido proceso) ha sido objeto de las más diversas interpretaciones, incluyendo las dadas en las constituciones proclamadas en la segunda mitad del Siglo XX, que le han dado contenido.

Incluso Séneca, en su ya clásico aforismo "nada se parece tanto a la injusticia como la justicia tardía", aludió a uno de los componentes que afectan el debido proceso; y actualmente, en

el Siglo XXI, con la sociedad de la información[12], el Estado constitucional tiene la oportunidad de evitar la situación descrita por el filósofo romano, al incorporar las TIC como medio determinante para evitar el colapso de los juzgados y su acumulación de asuntos, con las indebidas dilaciones que conllevan a la violación del debido proceso.

Si en el Siglo XVIII la Modernidad imponía la mecanización de tareas como base de la Revolución Industrial, en pleno Siglo XXI las transformaciones del Estado contemporáneo exigen la incorporación de las tecnologías a las estructuras públicas como mecanismo de eficacia.

"Digitalizar la Administración y la Justicia supone considerar la tecnología como un activo estratégico de primera magnitud, incorporar el nuevo paradigma tecnológico en la prestación de los servicios públicos" (Martín Rodrigo, 2001, s.p.); como afirmase Gascó Hernández (2001), "supone transformar la relación fundamental que existe entre el Gobierno y el público".

> No se trata de buscar la tecnología por la tecnología, ni la modernidad por la modernidad, sino de servir mejor a los ciudadanos. Si se olvidan estas y otras reglas se corre el peligro cierto de agrandar las brechas existentes en la sociedad (Arenilla Sáez, 2003, s.p.).

Como refiere Criado Grande (2010), el asunto no se circunscribe solo al paso de la Administración o la Justicia convencional en papel a medios digitales, sino que se trata de un proceso de mucho más alcance que involucra soluciones TIC, como he referido con anterioridad.

---

[12] Concepto acuñado por FRIEZ MACHLUP en 1961 y consagrado jurídicamente en la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información

5.3. La necesidad de un plan estratégico de ciberseguridad para la Fiscalía General de la Nación

Durante el desarrollo de este trabajo se ha señalado la necesidad de implementar una estrategia estructural de utilización de tecnologías de la información y las comunicaciones en la FGN, que la misma debe estar precedida de la elaboración de una arquitectura jurídica y técnica, que es fundamental incorporar en el marco de las investigaciones penales análisis de datos y técnicas de *big data*; así mismo, se ha hablado de que se requiere determinar una regulación pertinente y autónoma para la FGN en desarrollo de lo que se ha denominado expediente digital, entre otros elementos; y que sin el acompañamiento de una estrategia de ciberseguridad estos no tendrían sentido.

En este punto, y con solo efectos enunciativos y descriptivos, no limitativos, ni exhaustivos, me permito señalar una propuesta estructural de los elementos que debe contener el mentado plan estratégico.

5.3.1. Gobernanza.

La "buena gobernanza" según lo presenta (Cerrillo Martínez, 2007) se erige con base en los principios de participación, eficacia, coherencia, transparencia y rendición de cuentas, (último término conocido como *accountability*); dichas directrices marcan la pauta para las diferentes políticas públicas caracterizadas por un trato más cooperativo y consensuado hacia la ciudadanía, según lo señalé en mi texto de doctorado.

Bajo este concepto, es necesario el desarrollo, desde el nivel estratégico de la FGN, de un conjunto de principios, normas y valores, que enmarquen la política de ciberseguridad de la

institución. Allí se deberá establecer, además, quién es la autoridad que ejercerá el liderazgo, la estructura de la organización; las formas, procesos y procedimientos de coordinación al interior y al exterior de esta. Este funcionario determinará el esquema de prevención de los riesgos, el de gestión de los mismos, y proyectará cómo se articulan con las líneas estratégicas de la Fiscalía; por último, fijará el límite que se tiene frente a la capacidad de reacción en un escenario de confrontación.

5.3.2. Desarrollo de capacidades.

5.3.2.1. Especiales.

La estrategia debe incorporar un conjunto de medidas tendientes a la creación, mantenimiento y fortalecimiento de cuatro grupos: uno de prevención de riesgos; en segundo lugar, otro de gestión de riesgos; en tercera instancia, un grupo especial de reacción defensiva frente a escenarios de confrontación; por último, un grupo de cibercriminalidad, cuyo objetivo esencial es la investigación de ataques a la infraestructura crítica del Estado, incluida la de la FGN.

5.2.3.2. Formación.

La estrategia debe contar con un plan a corto, mediano y largo alcance que permita la formación, en los distintos niveles —básico, técnico, profesional, especializado y experto— del conjunto de servidores de la FGN, así como en el nivel de docentes y de estudiantes. De la misma manera, deben existir unos elementos mínimos de formación para los usuarios o ciudadanos que se relacionan con la entidad en el marco de la función constitucional.

Dicho plan de capacitaciones debe tener como principios la integralidad, transversalidad, permanencia, la prospectiva y la responsabilidad.

La estrategia deberá desarrollar el conjunto de planes, programas, centros y capacitación especializada que se deberá alinear con los objetivos estratégicos de la FGN, y cuyo objetivo final será una política clara de educación, capacitación y sensibilización frente a la ciberseguridad y ciberdefensa de la FGN.

5.2.3.3. Tecnológicas.

Dada la condición de infraestructura crítica, la FGN deberá contar con tecnología de punta que dé soporte a cuatro elementos:

El primero de ellos tiene que ver con el cumplimiento de la misión institucional, ello implica que los desarrollos tecnológicos deberán garantizar el cumplimiento del artículo 250 de la Constitución Política; el segundo tiene que ver con el soporte que se requiere para el cumplimiento de las funciones administrativas que, de forma excepcional, cumple la FGN.

El tercer componente se refiriere a una plataforma de *big data y analitycs* que permita la interrelación de la información y con ello se puedan tomar decisiones estratégicas en el marco del cumplimiento de las dos funciones anteriores y, por último, una estructura tecnológica, tipo Centro de Operaciones de Seguridad (en adelante: SOC, por sus siglas en inglés), para prevención, gestión de riesgos e incidentes y respuesta en caso de escenarios de confrontación.

5.3.3. Esquema para prevención del riesgo, gestión de incidentes y defensa de la infraestructura crítica en la Fiscalía.

En la estrategia será necesaria la incorporación de tres elementos específicos, señalándose en cada uno de ellos los procesos, procedimientos, responsables, responsabilidades, y esquemas de reacción que tengan que ver con los siguientes elementos:

En primera instancia, la prevención de los riesgos, esto es, todas las medidas humanas, técnicas, institucionales, personales, económicas y políticas, necesarias para la prevención de los riesgos.

En segundo lugar, tenemos la gestión de incidentes; se deben establecer las técnicas, procesos y procedimientos que se tendrán que desarrollar frente a un escenario en el que se vea comprometida la infraestructura física y lógica de la entidad.

Por último, se encuentra el conjunto de normas, procesos y procedimientos en caso de verse comprometida la infraestructura crítica de la entidad, es decir, la capacidad de reacción y sus límites en un escenario de confrontación.

Así las cosas, existe un elemento transversal que es el de señalar que la infraestructura física y lógica de la entidad es el corazón y cuáles son las capas en que se permite su intrusión y los niveles correspondientes.

5.3.4. Marco legal.

Siendo este uno de los elementos esenciales de la estrategia, en el desarrollo de este trabajo he identificado la necesidad de regular las siguientes situaciones de manera autónoma para la FGN:

Incorporación y desarrollo de la estrategia de gobierno digital para la fiscalía general, allí se deberá establecer: organización y funcionamiento; responsables y responsabilidades; fases de implantación; tiempos y obligaciones de cumplimiento frente a cada uno de las fases; vinculación jurídica y responsabilidades en gestión de riesgos, gestión de incidentes, cooperación, y límites de respuesta en escenarios de conflicto.

En cuanto al régimen jurídico se requiere:

- Régimen jurídico para identificación electrónica de ciudadanos, servidores públicos y sedes electrónicas.
- Régimen jurídico para el expediente judicial electrónico.
- Régimen jurídico para el esquema de interoperabilidad de los sistemas.
- Régimen jurídico para analítica, *big data* y protección de datos, a partir del uso de las informaciones de las investigaciones.
- Régimen jurídico para la protección de la infraestructura crítica de la FGN.

5.3.5. Marcos de cooperación y diplomacia.

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

5.3.6. Investigación, desarrollo e innovación.

Uno de los elementos más importantes que deberá abordar la estrategia de ciberseguridad y ciberdefensa es la creación de un centro de innovación y prospectiva en ciberseguridad para la Fiscalía General de la Nación; el objetivo esencial será estudiar, a partir de la convergencia de investigaciones públicas, privadas y militares, el fenómeno de la cibercriminalidad en contra de infraestructuras críticas en el marco de la Administración justicia. Aquí se plantea la creación de un centro de excelencia en ciberseguridad para la FGN.

Conclusiones

La investigación presentada en esta tesis ha dado lugar a concretar las siguientes conclusiones.

PRIMERA: el anterior análisis deja planteado un problema para desarrollar tanto tecnológica como jurídicamente, es decir, la utilización de las tecnologías de la información y las comunicaciones en la Administración de justicia como instrumento para la gestión y análisis en la investigación penal para la construcción de contexto y la generación de memoria. Lo anterior deja abiertos tres frentes de discusión: por un lado, la afectación a la cláusula de reserva que tienen las investigaciones en la fase inicial, a saber, los procesos seguidos por la Ley 600 de 2000 en su etapa previa, así como las investigaciones que se siguen por el procedimiento de Ley 906 de 2004 hasta la fase del descubrimiento probatorio; la segunda de las cuestiones es la necesidad de una estrategia autónoma, independiente e integradora para la utilización de las TIC en la Fiscalía General de la Nación; por último, la necesidad de una estrategia de ciberseguridad.

SEGUNDA: el otro aspecto es el relacionado con el tratamiento de los datos personales de los ciudadanos incursos en las investigaciones criminales, esto es, su tratamiento no debe superar la esfera de la finalidad, vale decir, de la investigación criminal en sí misma. En este sentido, cualquier tecnología que se incorpore para materializar la investigación a través de *big data* debe ser respetuoso de esa protección constitucional y debe garantizar el derecho a la intimidad. Así mismo, se requiere la delimitación del instrumento jurídico a través del cual se incorporan a los procesos, como prueba, los resultados de los análisis objetivos anteriores.

TERCERA: la sociedad demanda una Administración de justicia eficiente y eficaz, ante ello es fundamental aplicar nuevas formas de investigación criminal; es por esto que se plantea la utilización de técnicas de análisis de información y *big data* que permitan generar nuevos resultados en las investigaciones, aplicar contextos y servir como instrumento de verdad y memoria.

CUARTA: el conjunto normativo colombiano no contiene normas propias para la Fiscalía General de la Nación que tengan como finalidad la implementación de una estrategia de gobierno digital para el cumplimiento de su función misional, establecida en el artículo 250 de la Constitución Política. En consecuencia, no hay un soporte jurídico suficiente que permita la incorporación de TIC en la Administración de justicia y, de manera específica, en la Fiscalía, en los términos del parágrafo 1 del artículo 2 del Decreto 2573 de 2014, el cual establece que "La implementación de la estrategia de Gobierno en línea en las Ramas legislativa y Judicial, en los órganos de control, en los autónomos e independientes y demás organismos del Estado, se realizará bajo un esquema de coordinación y colaboración armónica en aplicación de los principios señalados en el artículo 209 de la Constitución Política".

QUINTA: es imperativo el desarrollo normativo —a partir de la arquitectura institucional— de las obligaciones, derechos, deberes, técnicas, procesos y procedimientos en servicios, gobierno abierto, gestión y seguridad, así como privacidad de la información. Por lo que se evidencia la necesidad de regulación, estructuración, desarrollo, incorporación, seguimiento y control del gobierno electrónico o digital en la FGN.

SEXTA: el desarrollo de actividades económicas, sociales, políticas y administrativas a través de las TIC trae riesgos asociados a la seguridad de la información, los cuales deben ser gestionados permanentemente. Los Estados, y de manera especial las administraciones públicas, entendidas como estructuras críticas, deben contar con una estrategia de seguridad de la información que tenga como pilar fundamental la gestión del riesgo. Del mismo modo, la integridad, autenticidad y disponibilidad de la información son elementos fundamentales en la generación de estrategias de ciberseguridad y por ende de ciberdefensa.

SÉPTIMA: la mala gestión de los riesgos llevaría a la materialización de amenazas o ataques cibernéticos, lo que tendría consecuencias sociales y económicas nefastas para los países y, en últimas, para los ciudadanos.

OCTAVA: un plan estratégico de ciberseguridad para la FGN debe contar con unas políticas claras en gobernanza, desarrollo de capacidades especiales, de formación y tecnológicas; igualmente, tiene que incluir un esquema para la prevención del riesgo, así como la gestión de los incidentes y defensa de la infraestructura crítica de la entidad. Este plan también debe contemplar un marco jurídico adecuado a las obligaciones de investigación y uso de TIC, al igual que una estructura de cooperación nacional e internacional clara, y un centro permanente de investigación, desarrollo e innovación.

NOVENA: la utilización de técnicas de análisis masivo de información será la herramienta con la que cuente la Administración pública electrónica para fundamentar las estrategias de ciberseguridad y ciberdefensa de los Estados; todas, en su conjunto, dentro del ámbito del cumplimiento del sistema normativo que permite la utilización de tecnologías en las propias

administraciones y el tratamiento de información y de datos en el marco del cumplimiento de sus funciones.

DÉCIMA: el conjunto de tecnologías que intervienen en una solución de *big data* se presenta como idóneo ante los retos de la Fiscalía General de la Nación; aquel incluye el análisis de contextos alimentados por un gran flujo de información dentro de la investigación criminal; por lo cual se hace urgente que el marco jurídico sea más específico para propiciar que se incluya dicha solución, que además da soporte a un sistema de ciberseguridad.

Referencias

Alvarez Carlos Enrique y otros (2017). *Seguridad y Defensa: conceptos en constante transformación.* ESDEGUE, recuperado de https://esdeguelibros.edu.co/index.php/editorial/catalog/book/27

Alemania, Tribunal Superior. Sala Civil. (enero de 24 de 2013). III ZR 98/12. *Compensación por la interrupción del servicio de internet "esencial para la vida".*

Alianza Caoba. (2017). *Centro de excelencia y apropiación*. Recuperado el 30 de abril de 2017, de http://alianzacaoba.co/

Arangüeña Fanego, C. (2010). Perspectivas de la e-justicia en Europa. En S. Coord: Montilla, *Presente y futuro de la e-justicia en España y la Unión Europea* (págs. 29-82). Cizur Menor, Navarra: Aranzadi.

Arenilla Sáez, M. (marzo-abril de 2003). El estado y la Administración pública en la sociedad de la información. *Boletín ASTIC*, 16-28. Recuperado el 14 de enero de 2017, de http://www.astic.es/sites/default/files/boletic_completos/boletic_25_2003_abril.pdf

Aucal Business School. (2016). *Ciberseguridad en la Unión Europea*. Recuperado el 3 de junio de 2017, de Ciberseguridad al día: http://www.ciberseguridadparaempresas.com/ciberseguridad-en-la-union-europea/

Audea.com. (2016). *Diferencias entre ciberseguridad y seguridad de la información*. Recuperado el 2017 de 3 de junio, de Audea: http://www.audea.com/es/diferencias-ciberseguridad-seguridad-la-informacion/

Barranco Fragoso, R. (2012). *¿Qué es big data?* Recuperado el 2 de junio de 2017, de IBM developerWorks: https://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/

Bellia, P. L. (2004). Surveillance Law Through Cyberlaw's Lens. *George Washington Law Review, 72*, 87. Recuperado el 22 de noviembre de 2017, de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=556467

Camargo Vega, J. J., Camargo Ortega, J. F., & Aguilar, L. J. (2015). Conociendo Big-Data. *Revista Facultad de Ingeniería, 24*(38), 63-77. Recuperado el 19 de enero de 2017, de http://revistas.uptc.edu.co/index.php/ingenieria/article/view/3159/4346

Castells, M. (2005). *La Era de la Información: economía, sociedad y cultura.* Madrid: La sociedad red, Alianza Editorial.

Cepal, Pnum. (2001). *Informe de la Conferencia Regional de América Latina y el Caribe Preparatoria de la Cumbre Mundial sobre el Desarrollo Sostenible.* Río de Janeiro. Recuperado el 16 de octubre de 2016, de https://www.cepal.org/publicaciones/xml/9/9289/lcg2173e.pdf

Cernada Badía, R. (24 de octubre de 2012). Los actos de comunicación electrónicos como instrumento de una efectiva tutela judicial. *(Trabajo de investigación, bajo la dirección de Cotino Lorenzo). Universidad de Valencia*. Valencia, España.

Cerrillo Martínez, A. (2007). E-justicia: las tecnologías de la información y el conocimiento al servicio de la justicia iberoamericana en el siglo XXI. *Revista de internet, derecho y política de UOC*(4). Recuperado el 23 de enero de 2017, de https://dialnet.unirioja.es/servlet/articulo?codigo=2254135

Chile, Ministerio - Secretaría General de la Presidencia. (2008). *Proyecto de Reforma y Modernización del Estado. Gobierno Electrónico en Chile Hoy.*

Clarke, R. A. (2011). *Ciberguerra.*

Colombia, C. d. (2011). *Ley 1474 de 2011, por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.* Bogotá: En Diario Oficial, núm. 48.128, 12 de julio de 2011. Recuperado el 17 de febrero de 2017, de http://programa.gobiernoenlinea.gov.co/apc-aa-files/92e2edae878558af042aceeafd1fc4d8/ley1474_2011.pdf

Colombia, Comisión de Regulación de Comunicaciones (CRC). (2014). *Informe de indicadores sectoriales e las TIC. Avance en la sociedad de la información n° 2.* Obtenido de http://colombiatic.mintic.gov.co/602/w3-article-6807.html

Colombia, Congreso de la República. (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: Diario Oficial, núm. 43.673, 21 de agosto de 1999. Recuperado el 11 de febrero de 2017, de http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

Colombia, Congreso de la República. (2000). *Ley 600 de 2000, por la cual se explide el Código de Procedimiento Penal.* Bogotá: En Diario Oficial, núm. 44.097, 24 de julio de 2000. Recuperado el 3 de febrero de 2017, de http://www.secretariasenado.gov.co/senado/basedoc/ley_0600_2000.html

Colombia, Congreso de la República. (2001). *Ley 1450 de 2011, por la cual se expide el Plan Nacional de Desarrollo, 2010-2014.* Bogotá: En Diario Oficial, núm. 48102, 16 de junio

de 2011. Recuperado el 11 de febrero de 2017, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=43101

Colombia, Congreso de la República. (2002). *Ley 790 de 2002, por la cual se expiden disposiciones para adelantar el programa de renovación de la Administración pública y se otorgan unas facultades extraordinarias al Presidente de la República.* Bogotá: En Diario Oficial, núm. 45.046, 27 de diciembre de 2002. Recuperado el 10 de febrero de 2017, de http://www.secretariasenado.gov.co/senado/basedoc/ley_0790_2002.html

Colombia, Congreso de la República. (2003). *Ley 812 de 2003, por la cual se aprueba el Plan Nacional de Desarrollo 2003-2006.* Bogotá: En Diario Oficial, núm. 45.231, 26 de junio de 2003. Recuperado el 20 de agosto de 2016, de http://programa.gobiernoenlinea.gov.co/apc-aa-files/92e2edae878558af042aceeafd1fc4d8/ley_812_2003.pdf

Colombia, Congreso de la República. (2004). *Ley 906 de 2004, por la cual se expide el Código de Procedimiento Penal.* Bogotá: En Diario Oficial, núm. 45.658, 1° de septiembre de 2004. Recuperado el 3 de febrero de 2017, de http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004.html

Colombia, Congreso de la República. (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: En Diario Oficial, núm. 46.023, 6 de septiembre de 2005 .

Colombia, Congreso de la República. (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: En Diario Oficial, núm. 46.023, 6 de septiembre de 2005. Recuperado el 6 de marzo de 2017, de http://www.secretariasenado.gov.co/senado/basedoc/ley_0962_2005.html

Colombia, Congreso de la República. (2005). *Ley 975 de 2005, por la cual se dictan disposiciones para la reincorporación de miembros de grupos armados organizados al margen de la ley, que contribuyan de manera efectiva a la consecución de la paz nacional y se dictan otras disposiciones para acuerdos humanitarios.* Bogotá: En Diario Oficial, núm. 45.980, 25 de julio de 2005. Recuperado el 3 de febrero de 2017, de http://www.secretariasenado.gov.co/senado/basedoc/ley_0975_2005.html

Colombia, Congreso de la República. (2007). *Ley 1147 de 2007, por la cual se adiciona la Ley 5ª de 1992 y se crean la Comisión Especial de Modernización y las Unidades Coordinadoras de Asistencia Técnica Legislativa y Atención Ciudadana del Congreso de la República.* Bogotá: En Diario Oficial, núm. 46.685,10 de julio de 2007. Recuperado el 16 de enero de 2017, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1147_2007.html

Colombia, Congreso de la República. (2007). *Ley 1147 de 2007, por la cual se adiciona la Ley 5ª de 1992 y se crean la Comisión Especial de Modernización y las Unidades Coordinadoras de Asistencia Técnica Legislativa y Atención Ciudadana del Congreso de la República.* Bogotá: En Diario Oficial, núm. 46.685, 10 de julio de 2007. Recuperado el 10 de marzo de 2017, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1147_2007.html

Colombia, Congreso de la República. (2007). *Ley 1151 de 2007, Plan de Desarrollo 2006 - 2010.* Bogotá: En Diario Oficial, Núm. 46.700, 25 de julio de 2007. Recuperado el 10 de febrero de 2017, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1151_2007.html

Colombia, Congreso de la República. (2009). *Ley 1341 de 2009, por a 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 de Espectro y se dictan otras disposiciones.* Bogotá: En Diario Oficial, núm. 47.426, 30 de julio de 2009. Recuperado el febrero de 20 de 2017, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html

Colombia, Congreso de la República. (2011). *Ley 1437 de 2011, por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo.* Bogotá: En Diario Oficial, núm. 47.956, 18 de enero de 2011. Recuperado el 3 de febrero de 2017, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1437_2011.html

Colombia, Congreso de la República. (2012). *Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.* Bogotá: En Diario Oficial, núm. 48.587, 18 de octubre de 2012. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Colombia, Congreso de la República. (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: En Diario Oficial, núm. 49.084, 6 de marzo de 2014. Recuperado el marzo de 2 de 2017, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html

Colombia, Congreso de la República. (2015). *Ley 1755 de 2015.* Bogotá: En Diario Oficial, núm. 49.559, 30 junio de 2015. Recuperado el marzo de 3 de 2017, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1755_2015.html

Colombia, Conpes. (2003). *Documento 3248. Renovación de la Administración pública.* Bogotá: Departamento Nacional de Planeación. Recuperado el agosto de 18 de 2017, de http://www.mintic.gov.co/portal/604/articles-3499_documento.pdf

Colombia, Conpes. (2010). *Documento 3649. Política nacional de servicio al ciudadano.* Bogotá: Departamento Nacional de Planeación. Recuperado el 3 de diciembre de 2016, de http://programa.gobiernoenlinea.gov.co/apc-aa-files/92e2edae878558af042aceeafd1fc4d8/conpes3649de2010.pdf

Colombia, Conpes. (2010). *Documento 3650. Importancia estratégica de la estrategia de gobierno en línea.* Bogotá: Departamento Nacional de Planeación. Obtenido de http://programa.gobiernoenlinea.gov.co/apc-aa-files/92e2edae878558af042aceeafd1fc4d8/conpes3650de2010.pdf

Colombia, Conpes. (2010). *Documento 3654. Política de rendición de cuentas de la rama ejecutiva a los ciudadanos.* Bogotá: Departamento Nacional de Planeación. Recuperado el 26 de mayo de 2017, de http://programa.gobiernoenlinea.gov.co/apc-aa-files/92e2edae878558af042aceeafd1fc4d8/conpes3654_2010.pdf

Colombia, Conpes. (2016). *Documento 3854. Política Nacional de Seguridad Digital.* Bogotá: Departamento Nacional de Planeación. Recuperado el 2 de junio de 2017, de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Colombia, Consejo Superior de la Judicatura (CSJud). (2012). *Acuerdo nº PSAA12-9269. Plan estratégico tecnológico para la rama judicial colombiana.* Bogotá: 27 de febrero de 2012. Obtenido de http://www.ramajudicial.gov.co/csj/noticias/csj/750/LaSala-Administrativa-adopta-el-Plan-Estrat%C3%A9gico-Tecnol%C3%B3gico-de-la-Rama-Judicial

Colombia, Consejo Superior de la Judicatura (CSJud). (2015). *Plan Sectorial de Desarrollo Rama Judicial 2015 - 2018.* Bogotá. Obtenido de https://www.ramajudicial.gov.co/documents/1513685/5113559/Plan_Sectorial_de_Desarrollo_Rama_Judicial_2015-2018+(3).pdf/a7b785e1-fb02-4ff6-905b-c16ac93df312

Colombia, Consejo Superior de la Judicatura. (2006). *Acuerdo No. PSAA06-3334 de 2006, por el cual se reglamentan la utilización de medios electrónicos e informáticos en el cumplimiento de las funciones de Administración de justicia.* Bogotá: En Gaceta de la Judicatura, 2 de marzo de 2006. Recuperado el 14 de febrero de 2017, de http://programa.gobiernoenlinea.gov.co/apc-aa-files/92e2edae878558af042aceeafd1fc4d8/ejus_csdj_2006_acuerdo_3334.pdf

Colombia, Constitución Política. (1991). Bogotá: Gaceta Constitucional No. 116. Recuperado el 30 de enero de 2017, de http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

Colombia, Corte Constitucional. (1999). *Sentencia de Constitucionalidad 923 con ponencia del Magistrado Álvaro Tafur Galvis.* Bogotá. Recuperado el 23 de abril de 2017, de http://ww.corteconstitucional.gov.co/RELATORIA/1999/C-923-99.htm

Colombia, Corte Constitucional. (2010). *Sentencia de Constitucionalidad 980 con ponencia del Magistrado Gabriel Eduardo Mendoza Martelo.* Bogotá. Recuperado el noviembre de 12 de 2016, de http://www.corteconstitucional.gov.co/relatoria/2010/c-980-10.htm

Colombia, Corte Constitucional. (2013). *Sentencia de Constitucionalidad 758 con ponencia del Magistrado Gabriel Eduardo Mendoza Martelo.* Bogotá. Recuperado el 27 de septiembre de 2016, de http://www.corteconstitucional.gov.co/RELATORIA/2013/C-758-13.htm

Colombia, Corte Constitucional. (2013). *Sentencia de Tutela 283 con ponencia del magistrado Jorge Ignacio Pretelt Chaljub.* Bogotá. Recuperado el 30 de septiembre de 2016, de http://www.corteconstitucional.gov.co/relatoria/2013/T-283-13.htm

Colombia, Corte Constitucional. (2014). *Sentencia de Constitucionalidad 034 con ponencia de la Magistrada María Victoria Calle Correa.* Bogotá. Recuperado el 29 de octubre de 2017, de http://www.corteconstitucional.gov.co/relatoria/2014/C-034-14.htm

Colombia, Fiscalía General de la Nación. (2013). *Manual del usuario del Sistema SPOA.* Recuperado el 10 de octubre de 2016, de http://web.fiscalia.col/fiscalnet/download/spoa/Manual%20de%20Usuario%20SPOA/Manual%20de%20Usuario%20Sistema%20SPOA.pdf

Colombia, Fiscalía General de la Nación. (2014). *Resolución 1343 de 2014, por la cual se reglamentan el Comité Nacional y los Comités Seccionales de Priorización de Situaciones y Casos, y se asignan diversas funciones para la implementación de la política de priorización.* Bogotá: 30 de julio de 2014. Recuperado el 4 de octubre de 2016, de http://www.fiscalia.gov.co/colombia/wp-content/uploads/Resoluci%C3%B3n-01343-de-2014-002.pdf

Colombia, 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 inve.* Recuperado el 21 de enero de 2017, de http://www.fiscalia.gov.co/colombia/priorizacion/priorizacion-nuevo-sistema-de-investigacion-penal/

Colombia, Fiscalía General de la Nación. (2015a). *Herramientas analíticas para la investigación y ejercicio de la acción penal. Cartilla 5.* Bogotá: Subdirección Nacional de Políticas Públicas. Recuperado el 4 de mayo de 2016, de http://www.fiscalia.gov.co/colombia/wp-content/uploads/CHP_Cartilla5_AF_Digital1.pdf

Colombia, Fiscalía General de la Nación. (2015b). *Construcción y análisis de indicadores de carga de trabajo. Cartilla 4.* Bogotá: Subdirección Nacional de Políticas Públicas. Recuperado el 3 de junio de 2016, de http://www.fiscalia.gov.co/colombia/wp-content/uploads/CHP_Cartilla4_AF_Digital1.pdf

Colombia, Fiscalía General de la Nación. (2016a). *Plan Estratégico 2016-2020. Fiscalía de la gente, para la gente y por la gente.* Bogotá. Recuperado el 18 de noviembre de 2016, de http://www.fiscalia.gov.co/colombia/wp-content/uploads/Plan-estrateigico-2016-2020-003-.pdf

Colombia, Fiscalía General de la Nación. (2016b). *La Fiscalía del Siglo XXI. Un camino hacia la modernización. 2012 - 2016.* Indicadores e informe de gestión, Bogotá. Recuperado el 10 de octubre de 2016, de http://www.fiscalia.gov.co/colombia/wp-content/uploads/Informe_Cuatrienio_corregido_2012-2016.pdf

Colombia, Fiscalía General de la Nación. (2017). *Resolución 738, por medio de la cual se aprueba el Direccionamiento Estratégico 2016-2020 para la Fiscalía General de la Nación.* Bogotá: 24 de febrero de 2017. Recuperado el 20 de marzo de 2017, de http://www.fiscalia.gov.co/colombia/wp-content/uploads/Direccionamiento-Estrat%C3%A9gico-2016-2020Vd.pdf

Colombia, Fiscalía General de la Nación. (s.f.a.). *Misión FGN.* Recuperado el 2017 de marzo de 20, de fiscalia.gov.co: http://www.fiscalia.gov.co/colombia/la-entidad/mision/

Colombia, Fiscalía General de la Nación. (s.f.). *Visión FGN.* Recuperado el marzo de 23 de 2017, de s.f.b.: http://www.fiscalia.gov.co/colombia/la-entidad/vision/

Colombia, Fiscalía General de la Nación. Unidad de Análisis y Contextos. (2013). Informe de rendición de cuentas 2012-2013. *Innovación en la investigación penal*, 75. Recuperado el 13 de noviembre de 2016, de http://www.fiscalia.gov.co/colombia/wp-content/uploads/Informe-rendici%C3%B3n-de-cuentas-UNAC-2012-2013.pdf

Colombia, Grupo de Respuesta a Emergencias Cibernéticas de Colombia (Colcert). (2013). *www.colcert.gov.co*. Recuperado el 22 de enero de 2016

Colombia, Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC). (2014). *Estrategia Gobierno en línea. 2012 - 2015 para el orden nacional. 2012 - 2017 para el orden territorial.* Bogotá. Recuperado el 2016 de 29 de noviembre, de http://programa.gobiernoenlinea.gov.co/apc-aa-files/eb0df10529195223c011ca6762bfe39e/manual-3.1.pdf

Colombia, Ministerio de Tecnologías de la Información y las Comunicaciones - Min TIC. (2014). *Innovación Nodo Justicia.* Bogotá: Sistema de investigación, desarrollo e innovación. Subsistema de innovación para el uso y apropiación de Tic en el Gobierno.

Colombia, P. d. (2012). *Decreto 19 de 2012, por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.* Bogotá: En Diario Oficial, núm. 48308, 10 de enero de 2012. Obtenido de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=45322

Colombia, Presidencia de la República. (1995). *Decreto 2150. Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública.* Bogotá: En Diario Oficial, núm. 42.137, 6 de diciembre de 1995. Recuperado el

17 de abril de 2017, de http://www.secretariasenado.gov.co/senado/basedoc/decreto_2150_1995.html

Colombia, Presidencia de la República. (2000). *Directiva presidencial No. 2.* Recuperado el 22 de abril de 2017, de http://programa.gobiernoenlinea.gov.co/apc-aa-files/92e2edae878558af042aceeafd1fc4d8/directiva_02_2000.pdf

Colombia, Presidencia de la República. (2001). *Decreto 127 de 2001. Por el cual se crean las Consejerías y Programas Presidenciales en el Departamento Administrativo de la Presidencia de la República.* Bogotá: En Diario Oficial, núm. 44.503, de 30 de julio de 2001. Obtenido de http://programa.gobiernoenlinea.gov.co/apc-aa-files/92e2edae878558af042aceeafd1fc4d8/decreto127de2001.pdf

Colombia, Presidencia de la República. (2002). *Directiva presidencial No. 10. Programa de Renovación de la Administración Pública: Hacia un Estado Comunitario.* Bogotá. Recuperado el 18 de abril de 2016, de http://programa.gobiernoenlinea.gov.co/apc-aa-files/92e2edae878558af042aceeafd1fc4d8/directiva_10_2002.pdf

Colombia, Presidencia de la República. (2003). *Decreto 3107 de 2003, por el cual se suprime un programa presidencial.* Bogotá: En Diario Oficial, núm. 45.357, 31 de octubre de 2003. Recuperado el 20 de abril de 2017, de http://www.mintic.gov.co/portal/604/articles-3599_documento.pdf

Colombia, Presidencia de la República. (2005). *Decreto 4669 de 2005, por el cual se reglamenta parcialmente la Ley 962 de 2005.* Bogotá: En Diario Oficial, núm 46.130, diciembre 22 de 2005. Recuperado el 2017 de febrero de 2016, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=18630#0

Colombia, Presidencia de la República. (2012). *Directiva Presidencia No. 04. Eficiencia administrativa y lineamientos de la política cero papel en la Administración pública.* Bogotá: En Diario Oficial, núm. 48.392, 3 de abril de 2012. Recuperado el 20 de abril de 2017, de https://www.mintic.gov.co/portal/604/articles-3647_documento.pdf

Colombia, Presidente de la República. (1999). *Decreto 1122 de 1999, por el cual se dictan normas para suprimir trámites, facilitar la actividad de los ciudadanos, contribuir a la eficiencia y eficacia de la Administración Pública y fortalecer el principio de la buena fe.* Bogotá: En Diario Oficial, núm. 43622, junio 29 de 1999. Recuperado el 10 de febrero de 2017, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=9208

Colombia, Presidente de la República. (2000). *Directiva Presidencial No. 02. Gobierno en línea.* Bogotá. Recuperado el 3 de marzo de 2017, de https://www.mintic.gov.co/portal/604/articles-3646_documento.pdf

Colombia, Presidente de la República. (2002). *Directiva Presidencial 10. Programa de Renovación de la Administración Pública: Hacia un Estado Comunitario.* Bogotá. Recuperado el 20 de febrero de 2017, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=5904

Colombia, Presidente de la República. (2008). *Decreto 1151 de 2008, por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.* Bogotá: En Diario Oficial, núm. 46960, abril 14 de 2008. Recuperado el 15 de septiembre de 2016, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=29774

Colombia, Presidente de la República. (2009). *Decreto 2623 de 2009.* Bogotá: En Diario Oficial, núm. 47.409, 13 de julio de 2009. Recuperado el 2 de abril de 2017, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36842

Colombia, Presidente de la República. (2012). *Decreto 19 de 2012, por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.* Bogotá: En Diario Oficial, núm. 48.308, 10 de enero de 2012. Recuperado el 30 de enero de 2017, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=45322

Colombia, Presidente de la República. (2012). *Directiva Presidencial 4. Eficiencia administrativa y lineamientos de la política cero papel en la Administración Pública.* Bogotá. Recuperado el marzo de 20 de 2017, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=50155

Colombia, Presidente de la República. (2014). *Decreto 2573 de 2014, por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.* Bogotá: En Diario Oficial, núm. 49363, 12 de diciembre de 2014. Recuperado el 10 de octubre de 2016, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60596#14

Colombia, Presidente de la República, Ministerio de Justicia y del Derecho. (1995). *Decreto 2150 de 1995, por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública.* Bogotá: En Diario Oficial, núm. 42.137, 6 de diciembre de 1995. Recuperado el 20 de febrero de 2017, de http://www.secretariasenado.gov.co/senado/basedoc/decreto_2150_1995.html

Colombia, Procuraduría General de la Nación. (2009). *Circular No. 58. Cumplimiento Decreto 1151 del 14 de abril de 2008.* Bogotá. Recuperado el 3 de febrero de 2017, de http://programa.gobiernoenlinea.gov.co/apc-aa-files/92e2edae878558af042aceeafd1fc4d8/circular_58_2008.pdf

Comisión Europea. (2003). *Comunicación de la Comisión al Consejo, al Parlamento europeo , al Comité Económico y Social Europeo y al Comité de las Regiones - El papel de la Administración electrónica en el futuro de Europa.* Bruselas: En documento 52003DC0567. COM/2003/0567 final. Recuperado el 17 de abril de 2017, de http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52003DC0567

Comisión Europea. (2007a). Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones. *Hacia una Política de lucha contra la ciberdelincuencia.* Bruselas: En Documento 52007DC0267. COM(2007) 267 final. Recuperado el 18 de enero de 2017, de http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52007DC0267

Comisión Europea. (2007b). *Programa europeo para la protección de infraestructuras críticas. Síntesis de la Comunicación de la Comisión.* Bruselas: COM (2006) 786 final en Diario Oficial C 126, 7 de junio de 2007. Recuperado el 19 de abril de 2017, de http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:l33260

Comisión Europea. (2008). *Comunicación de la Comisión al Consejo, al Parlamento Europeo y al Comité Económico y Social Europeo - Hacia una estrategia europea en materia de e-justicia (Justicia en línea).* Bruselas. Recuperado el 22 de noviembre de 2016, de http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52008DC0329&from=ES

Comisión Europea. (2010). Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. *Garantizar el Espacio*

de libertad, seguridad, y justicia para los ciudadanos europeos. Plan de Acción por el que se aplica el Programa de Estocolmo. Bruselas: En Documento 52010DC0171. COM(2010) 171 final. Recuperado el 18 de enero de 2017, de http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52010DC0171

Comisión Europea. (s.f.). *ventanilla única en e-justicia*. Recuperado el 20 de octubre de 2016, de https://e-justice.europa.eu/home.do?action=home&plang=es.

Consejo Argentino para las Relaciones Internacionales, CARI. (2013). *Ciberdefensa-Ciberseguridad. Riesgos y amenazas.* Recuperado el 17 de abril de 2017, de http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf

Consejo Europeo. (2008). *Plan de Acción Plurianual 2009-2013 relativo a la Justicia en red europea del Consejo.* Aprobado el 28 de noviembre de 2008 (DOUE C 75 de 31 de marzo de 2009). Obtenido de "http://eur-europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:075:0001:0012:ES:PDF

Cotino Hueso, L. (2003). La Administración y gobierno electrónico s en los documentos institucionales básicos de la sociedad de la información. En *Actas del XVII Congreso de Derecho e informática* (págs. 257-289). Madrid: Universidad de Comillas, U. Comillas-Instituto de Informática Jurídica.

Cotino hueso, L. (2012). El derecho a relacionarse electrónicamente con las Administraciones y el estatuto del ciudadano e-administrado en la Ley 11/2007 y la normativa de desarrollo. En E. (Coords) Gamero Casado, & J. Valero Torrijos, *Las tecnologías de la información y la comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio* (págs. 177-344). Cizur Menor, Navarra: Thomson Reuters-Aranzadi.

Cotino Hueso, L. (2013). Derecho y gobierno abierto. En J. Bermejo Latre, & S. Castel Gayán, *Transparencia, participación ciudadana y Administración pública en el Siglo XXI. Monografía Revista Aragonesa de Administración Pública.* Zaragoza.

Criado Grande, J. I. (2010). *Entre sueños utópicos y visiones pesimistas. Internet las TIC en la modernización de las Administraciones públicas* (Premio INAP ed.). INAP.

Dans, E. (2011). Big Data: una pequeña introducción. [Entrada de blog]. *enriquedans.com*. Recuperado el 20 de noviembre de 2016, de https://www.enriquedans.com/2011/10/big-data-una-pequena-introduccion.html

de Carlos Izquierdo, J. (2016). *La nueva estrategia de seguridad europea 2016.* Instituto Español de Estudios Estratégicos (IEEE) - Ministerio de Defensa de España . Recuperado el 3 de abril de 2016, de http://www.ieee.es/Galerias/fichero/docs_marco/2016/DIEEEM16-2016_EstrategiaSeguridad_DeCarlos.pdf

de Hoyos Sancho, M. (2008). Hacia un proceso civil más eficiente: comunicaciones telemáticas. El sistema "Lexnet". En F. Coord: Carpi, & M. P. Ortells Ramos, *Oralidad y escritura e un proceso civil eficiente* (pág. 94). Valencia: Universidad de Valencia.

Delgado García, A. M., & Oliver Cuello, R. (2006). *Las tecnologías de la información y la comunicación en la Administración de Justicia.* Oñati: IVAP.

Delgado, R., Vargas de Roa, R. M., Vives, M., Luque, P., Lara, L., & Arias, R. (2005). *Educación para el conocimiento social y político. Estado del arte* (Primera ed.). Facultad de Educación. Pontificia Universidad Javeriana.

DiazGranados, G. (2016). La comercialización del big data. Big data and commercial law. *Revista Universitas Estudiantes. Universidad Javeriana*(14), 111-128. Recuperado el 3 de junio de 2017, de

http://cienciasjuridicas.javeriana.edu.co/documents/3722972/7912168/7-LA+COMERCIALIZACI%C3%93N.pdf/17c8d327-d25b-474c-a9c1-1797114e3c0b

El mercado del Big Data crecerá hasta los 32.400 millones de dólares en 2017. (2013). *computerworld*. Recuperado el 23 de enero de 2017, de http://www.computerworld.es/sociedad-de-la-informacion/el-mercado-del-big-data-crecera-hasta-los-32400-millones-de-dolares-en-2017

Endsley, M. R., Tecnologies, S., & Garland, D. J. (2000). Theoretical underpinnings of situation awareness: A critical review. *Situation Awareness Analysis And Measurement*, 1-24. Recuperado el 22 de octubre de 2016, de http://www.scs.ryerson.ca/aferworn/courses/CP8306/CLASSES/CP8306CL03/SATheory chapter.pdf

España, Agenda Digital para España. (s.f.). *Plan Avanza*. Recuperado el 10 de marzo de 2017, de http://www.agendadigital.gob.es/agenda-digital/planes-anteriores/Paginas/plan-avanza.aspx

España, Consejo General del Poder Judicial. (2005). *Acuerdo de 15 de septiembre de 2005, del Pleno del Consejo General del Poder Judicial, por el que se aprueba el Reglamento 1/2005, de los aspectos accesorios de las actuaciones judiciales.* Madrid: En Boletín Oficial del Estado, núm. 231, 27 de septiembre de 2005. BOE-A-2005-15939. Recuperado el 18 de febrero de 2017, de https://www.boe.es/buscar/doc.php?id=BOE-A-2005-15939

España, Consejo General del Poder Judicial. (2006). *Acuerdo de 20 de septiembre de 2006, del Pleno del Consejo General del Poder Judicial, de creación de ficheros de carácter personal dependientes de los órganos judiciales.* Madrid: En Boletín Oficial del Estado,

núm. 244, 12 de octubre de 2006. BOE-A-2006-17867. Recuperado el 3 de marzo de 2017, de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2006-17867

España, Consejo General del Poder Judicial. (2008). *Acuerdos del Pleno del CGPJ de 12 de noviembre de 2008.* Recuperado el 10 de febrero de 2017, de Poder Judicial de España: http://www.poderjudicial.es/portal/site/cgpj/menuitem.65d2c4456b6ddb628e635fc1dc432ea0/?vgnextoid=7ae2f93850fbe210VgnVCM1000006f48ac0aRCRD&vgnextfmt=default&vgnextlocale=es_ES

España, Jefatura de Estado. (2003). *Real Decreto 937/2003, de 18 de julio, de modernización de los archivos judiciales.* Madrid: En Boletín Oficial del Estado, núm. 181, 30 de julio de 2003. BOE-A-2003-15237.

España, Jefatura del Estado. (1985). *Ley Orgánica 6 de 1985.* Madrid: En Boletín Oficial del Estado, núm. 157, 2 de julio de 1985. Recuperado el 3 de marzo de https://www.boe.es/buscar/doc.php?id=BOE-A-1985-12666

España, Jefatura del Estado. (1992). *Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.* Madrid: En Boletín Oficial del Estado, núm. 285, 27 de Noviembre de 1992. Recuperado el 18 de enero de 2017, de http://noticias.juridicas.com/base_datos/Admin/l30-1992.html

España, Jefatura del Estado. (1994). *Ley Orgánica 16/1994, de 8 de noviembre, por la que se reforma la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.* Madrid: En Boletín Oficial del Estado, núm. 268, de 9 de noviembre de 1994. BOE-A-1994-24612. Recuperado el 20 de enero de 2017, de https://www.boe.es/buscar/doc.php?id=BOE-A-1994-24612

España, Jefatura del Estado. (2007). *Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.* Madrid: En Boletín Oficial del Estado. Recuperado el 17 de enero de 2017, de http://noticias.juridicas.com/base_datos/Admin/l11-2007.html

España, Jefatura del Estado. (2009). *Ley 13/2009, de 3 de noviembre, de reforma de la legislación procesal para la implantación de la nueva Oficina judicial.* Madrid: En Boletín Oficial del Estado, núm. 266, 4 de noviembre de 2009. BOE-A-2009-17493. Recuperado el 2 de febrero de 2017, de https://www.boe.es/buscar/doc.php?id=BOE-A-2009-17493

España, Jefatura del Estado. (2011). *Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.* Madrid: En Boletín Oficial del Estado, núm. 160, 6 de julio de 2011. BOE-A-2011-11605. Recuperado el 4 de febrero de 2017, de https://www.boe.es/buscar/doc.php?id=BOE-A-2011-11605

España, Jefatura del Estado. (2011). *Ley 8 de 2011 por la que se establecen medidas para la protección de las infraestructuras críticas.* Madrid: En Boletín Oficial del Estado (BOE) Legislación consolidada, núm 102, 28 de abril de 2011. Recuperado el 4 de febrero de 2017, de https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf

España, Ministerio de Justicia. (1999). *Orden de 19 julio de 1999 sobre informatización de los Registros civiles.* Madrid: Boletón Oficial del Estado, núm 180, 29 de julio de 1999. BOE-A-1999-16537. Recuperado el 20 de febrero de 2017, de https://www.boe.es/buscar/doc.php?id=BOE-A-1999-16537

España, Ministerio de Justicia. (2007). *ORDEN JUS/1468/2007, de 17 de mayo, sobre impulso a la informatización de los registros civiles y digitalización de sus archivos.* Madrid: En

Boletín Oficial, núm. 128, 29 de mayo de 2007. Recuperado el febrero de 23 de 2017, de https://www.boe.es/buscar/doc.php?id=BOE-A-2007-10702

España, Ministerio de Justicia. (2007). *ORDEN JUS/1468/2007, de 17 de mayo, sobre impulso a la informatización de los registros civiles y digitalización de sus archivos.* Madrid: Boletín Oficial del Estado, núm. 128, 29 de mayo de 2007. BOE-A-2007-10702. Recuperado el 10 de febrero de 2017, de https://www.boe.es/buscar/doc.php?id=BOE-A-2007-10702

España, Ministerio de Justicia. (2009). *Plan Estratégico de Modernización de la Justicia 2009-2012.* Recuperado el 30 de enero de 2017, de mjusticia.es: https://www.mjusticia.es/estatico/cs/mjusticia/pdf/PEModernizacion2009_2012.pdf

España, Ministerio de Justicia (2007). *Real Decreto 84/2007, sobre implantación en la Administración de Justicia del sistema informático de telecomunicaciones Lexnet para la presentación de escritos y docs, el traslado de copias y la realización de act. de com. procesal por medios telemáticos.* (2007). Madrid: En Boletín Oficial del Estado, núm. 38, 13 de febrero de 2007. BOE-A-2007-2954. Recuperado el 20 de febrero de 2017, de https://boe.es/diario_boe/txt.php?id=BOE-A-2007-2954

España, Ministerio de Justicia. (2009). *Real Decreto 95/2009, de 6 de febrero, por el que se regula el Sistema de registros administrativos de apoyo a la Administración de Justicia.* Madrid: En Boletín Oficial el Estado, núm. 33, 7 de febrero de 2009. BOE-A-2009-2073. Recuperado el 2 de febrero de 2017, de https://www.boe.es/buscar/act.php?id=BOE-A-2009-2073

España, Ministerio de Justicia. (2012). *Pla de Acción 2012 - 2015. Secretaría General de la Administración de Justicia.* Madrid. Recuperado el febrero de 22 de 2017, de http://www.mjusticia.gob.es/cs/Satellite/Portal/1292427277121?blobheader=application

%2Fpdf&blobheadername1=Content-Disposition&blobheadervalue1=attachment%3B+filename%3DPlan_de_Accion_de_la_SGAJ_

Esparza Leibar, I. (1995). *El principio del proceso debido.* Barcelona: J.M. Bosh.

Estados Unidos de América. (2009). *Computer Crime & Intellectual Property Section.* Recuperado el 18 de noviembre de 2016, de https://www.justice.gov/criminal-ccips

European Council. (2007). *Report by the council working party on legal data processing (E-justice).* Bruselas: Document 10393/07. Jurinfo. JAI 293. Justiciv 159. Copen 86. Recuperado el 17 de octubre de 2016, de http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010393%202007%20INIT

Fases en big data y librerías hadoop. (s.f.). Recuperado el 10 de abril de 2017, de hop2croft's software development Blog: https://hop2croft.wordpress.com/2013/08/28/fases-en-big-data-y-librerias-hadoop/

Fernández Gómez, L. (2014). *¿Cómo puede el gobierno colombiano aprovechar de mejor manera el potencial de big data?* Ministerio TIC, Dirección de Gobierno en Línea. Documento de investigación en el marco del programa Talento Digital, a partir de la investigación entregada a la Universidad de Manchester para el grado de Maestría en TIC para el Desarrollo. Recuperado el 2017 de abril de 19, de http://centrodeinnovacion.gobiernoenlinea.gov.co/sites/default/files/documento_investigacion_mintic.pdf

Fernández, R. (2009). Estonia, primera víctima de los 'hackers'. Un contencioso con Rusia desencadenó la paralización digital del país en 2007. *El País*. Recuperado el 29 de enero de 2017, de https://elpais.com/diario/2009/05/30/internacional/1243634402_850215.html

Fuerzas Militares de Colombia, Ejército Nacional. (2015). *Procedimiento comunicaciones operacionales y ciberdefensa.* Recuperado el 18 de abril de 2017, de https://www.ejercito.mil.co/?idcategoria=357574&download=Y

Fundación Telefónica. (2014). *La Sociedad de la Información en España 2013.* Madrid: Ariel. Recuperado el 18 de abril de 2017, de https://www.fundaciontelefonica.com/arte_cultura/publicaciones-listado/pagina-item-publicaciones/itempubli/261/

Fundación Telefónica. (2017). *La Sociedad de la Información en España 2016.* Ariel. Recuperado el 24 de abril de 2017, de https://www.fundaciontelefonica.com/arte_cultura/publicaciones-listado/pagina-item-publicaciones/itempubli/558/

Gallardo, M. G. (2013. Julio, 31). Los 6 pasos que su organización debe seguir para confiar en Big Data. *CIO América Latina*. Recuperado el 5 de febrero de 2017, de Cio América Latina: http://www.cioal.com/2013/07/31/los-6-pasos-que-su-organizacion-debe-seguir-para-confiar-en-big-data/

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 E. Gamero Casado, & J. Valero Torrijos, *Las tecnologías de la información y la comunicación en la Administración de Justicia. Análisis sistemático de la ley 18/2011, de 5 de julio* (págs. 45-88). Cizur Menor, Navarra: Thomson Reuters-Aranzadi.

Gartner. (2013). *Big data.* Recuperado el 17 de abril de 2017, de gartner.com: http://www.gartner.com/it-glossary/big-data/

Gartner Inc. (2012). *Reporte Gartner analiza "big data" alrededor de tecnología de datos.* Recuperado el 18 de noviembre de 2016, de http://searchdatacenter.techtarget.com/es: http://searchdatacenter.techtarget.com/es/noticias/2240171952/Reporte-de-Gartner-analiza-big-data-alrededor-de-tecnologia-de-datos

Gascó Hernández, M. (2001). *Una aproximación a la definición de políticas de inserción en la sociedad de la información.* VI Conferencia CLAD.

Gascón, F. (2010). La e-justicia en la Unión europea: Balance de situación y planes para el futuro (en diciembre de 2009). En C. Senes Montilla [coord.], *Presente y futuro de la e-justicia en España y la Unión Europea* (págs. 83-125). Cizur Menor (Navarra): Aranzadi.

Gobierno en Línea, Ministerio de Comunicaciones, Universidad de los Andes. (2009). *Metodología de monitoreo de Gobierno en Línea.* Bogotá. Recuperado el 29 de abril de 2017, de http://programa.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/GEL_MetodologiaMonitoreoEvaluacionGEL.pdf

Gómez, H. (31 de enero de 2014). Oracle apuesta por Big Data con tecnología y proyectos. *Dealer World.* Recuperado el 18 de enero de 2017, de http://www.dealerworld.es/actualidad/oracle-apuesta-por-big-data-con-tecnologia-y-proyectos

González, A. (2014). ¿Qué es machine learning? *Clever Data, big data prediction. A clever task company.* Recuperado el 3 de junio de 2017, de http://cleverdata.io/que-es-machine-learning-big-data/

Hinestrosa Vélez, J. P. (2013). Construcción de contextos en la aplicación de la Ley 1448 de 2011. *Seminario Internacional. Importancia de la construcción de contextos en las*

investigaciones judiciales (págs. 40-46). Bogotá: Fiscalía General de la Nación. Unidad de Análisis y Contextos (UNAC). Recuperado el 18 de enero de 2017, de http://www.fiscalia.gov.co/colombia/wp-content/uploads/Seminario-Internacional-Construcci%C3%B3n-de-Contextos.pdf

ICDE. (s.f.). *Avances de big data en el sector público colombiano*. Recuperado el 3 de junio de 2017, de Infraestructura Colombiana de Datos Espaciales (ICDE): http://www.icde.org.co/noticias/Avances-De-Big-Data-En-El-Sector-Publico-Colombiano

Informe Freedomhouse. (2014). *Freedom House Publicaciones*. Recuperado el 27 de abril de 2017, de https://freedomhouse.org/publicaciones

Internet World Stats. Usage and Population Satatics. (s.f.). Recuperado el 2 de octubre de 2016, de http://www.internetworldstats.com/stats.htm

internetworldstats. (2012). Recuperado el 2 de octubre de 2016, de http://www.internetworldstats.com/stats.htm

ITU. (2012). *StatisTIC*. Recuperado el 3 de octubre de 2016, de http://www. itu. int/ict/statisTIC

ITU Statics. (2016). *Data for the world*. Recuperado el 3 de enero de 2017, de Key 2005-2016.

Kosutic, D. (2012). *Ciberseguridad en 9 pasos. Manual sobre seguridad de la información para el gerente.* (G. Trentini, Trad.) Zagreb: EPPS Services Ltd. ISBN: 978-953-57452-2-8. Recuperado el 10 de abril de 2017, de https://advisera.com/wp-content/uploads/sites/9/2016/09/Ciberseguridad_en_9_pasos_ES.pdf

Llamas Fernández, M., y Gordillo Luque, J. M. (2007). Medios técnicos de vigilancia. En E. Velasco Núñez, *Los nuevos medios de investigación en el proceso penal: especial referencia a la tecnovigilancia.* España: Consejo General del Poder Judicial.

López, J. J. (2014). Las principales Técnicas Big Data y sus Aplicaciones. *Ideas de un Project Manager – José Julio López*. Recuperado el 16 de abril de 2017, de https://josejuliolopezsantos.wordpress.com/2014/07/11/las-principales-tecnicas-big-data-y-sus-aplicaciones/

Machín, N., & Gazapo, M. (2016). La ciberseguridad como factor crítico en la seguridad de la Unión Europea. *Revista Unisci*(42), 47-68. Recuperado el 15 de abril de 2017, de http://revistas.ucm.es/index.php/RUNI/article/view/53786/49258

Martín Rodrigo, T. (2001). Proyecto para una Administración electrónica en España. *Revista del CLAD Reforma y Democracia*(20), 1-17.

Martínez Osorio, D. (2013). Investigación de contexto y crímenes de sistema. *Seminario internacional. Importancia de la construcción de contexos en la investigaciónes judiciales* (págs. 31-33). Bogotá: Fiscalía General de la Nación. Unidad de Análisis y Contextos (UNAC). Recuperado el 20 de enero de 2017, de http://www.fiscalia.gov.co/colombia/wp-content/uploads/Seminario-Internacional-Construcci%C3%B3n-de-Contextos.pdf

Martínez Soria, J. (2006). gobierno electrónico en Alemania y en Europa. En L. Cotino Hueso, *Democracia, participación y voto a través de las nuevas tecnologías* (Colección Sociedad de la Información° 13 ed., págs. 245-262). Comares, Granada.

Ministerio de Defensa, Instituto Español de Estudios Estratégicos (IEEE). (2012). *El ciberespacio. Nuevo escenario de confrontación* (Colecciones: Monografías del CESEDEN ed.). España: Centro Superior de Estudios de la Defensa Nacional. ISBN: 978-84-9781-724-0. Recuperado el 16 de abril de 2017, de https://dialnet.unirioja.es/servlet/libro?codigo=547632

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). *Colombia sigue avanzando en indicadores de la Sociedad de la Información*. Recuperado el 22 de noviembre de 2016, de http://colombiatic.mintic.gov.co/602/w3-article-6807.html

Ministerio de Tecnologías de la Información y las Comunicaciones. (s.f.). *Big data.* Recuperado el 17 de abril de 2017, de IDI: Investigación, desarrollo e innovación: http://www.mintic.gov.co/portal/604/w3-article-6163.html

Mora, L. (2016). Qué es big data: fases y elementos. *Ve.* Recuperado el 17 de abril de 2017, de https://www.ve.com/es/blog/que-es-big-data-fases-elementos

Mutter, K. W. (2006). Propiedad intelectual y desarrollo en Colombia. *Revista Estudios Socio-Jurídicos, 8*(2). Recuperado el 25 de mayo de 2016, de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0124-05792006000200004#num19

Naciones Unidas (ONU), oficina contra la droga y el delito. (2010). *Sistemas policiales de información e inteligencia, Manual de Instrucciones para la evaluación de la justiica penal.* Nueva York: UNODC.

Organización de Estados Americanos, OEA. (2013). *Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos.* Trend Micro. Recuperado el 19 de abril de 2017, de https://www.sites.oas.org/cyber/Documents/2013%20-%20Tendencias%20en%20la%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe%20y%20Respuestas%20de%20los%20Gobiernos.pdf

Organización de Estados Americanos, OEA. (2015). *Iniciativa de seguridad cibernética de la OEA. Foro global de experticia cibernética (GFCE).* Recuperado el 18 de abril de 2017,

de https://www.sites.oas.org/cyber/Documents/2015%20Iniciativa%20de%20Seguridad%20Cibern%C3%A9tica%20de%20la%20OEA.PDF

Organization of American States, OAS. (2016). *Cybersecurity. Are we ready in Latin America and the Caribbean?* Recuperado el 18 de abril de 2017, de https://www.sites.oas.org/cyber/Documents/2016%20-%20Informe%20Ciberseguridad%202016%20Estamos%20preparados%20America%20Latina%20y%20el%20Caribe-Belisario%20Contreras,%20OEA.pdf

Ortiz Pradillo, J. C. (2013). *La investigación del delito en la era digital. Los derechos fundamentales frente a las nuevas medidas tecnológicas de la investigación.* Fundación Alternativas. Recuperado el 20 de noviembre de 2016, de http://www.fundacionalternativas.org/public/storage/actividades_descargas/5a687574bb9f245b66286372359596d4.pd

Ortoll, E. (2014). Big data se escribe con V. *COMeIN Revista de los Estudios de Ciencias de la Información y de la Comunicación*(37). Recuperado el 1° de junio de 2017, de http://comein.uoc.edu/divulgacio/comein/es/numero37/articles/Article-Eva-Ortoll.html

Palacios, P., Delgado, E., León, E., Montaño, J., & Estupiñán, A. (2014). Sistemas de información bibliográficos como estrategia para la disposición y acceso al conocimiento para la salud en Colombia. *Revista Monitor Estratégico. Superintendencia Nacional de Salud*(5), 81-88. Recuperado el 3 de junio de 2017, de https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/IA/SSA/Articulo%2011.pdf

Parlamento Europeo (PE) y Consejo de la Unión Europea (Consejo). (2000). *Directiva 2000/31/CE relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).* Luxemburgo: En Diario Oficial de las Comunidades Europeas, L 178, 17 de julio de 2000. Recuperado el 21 de enero de 2017, de http://www.wipo.int/edocs/lexdocs/laws/es/eu/eu107es.pdf

Parlamento Europeo (PE) y Consejo de la Unión Europea (Consejo). (2006). *Reglamento (CE) núm. 1896/2006, por el que se establece un proceso monitorio europeo que, entre otras medidas, permite la notificación del requerimiento de pago por medios electrónicos.* Luxemburgo: 12 de diciembre de 2006.

Parlamento Europeo (PE) y Consejo de la Unión Europea (Consejo). (2007). *Reglamento (CE) núm. 861/2007 por el que se establece un Proceso de escasa cuantía diseñado para su empleo directo por consumidores y por los pequeños empresarios.* Luxemburgo: 11 de julio de 2007.

Parlamento Europeo (PE) y Consejo de la Unión Europea (Consejo). (2016). *Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y.* Estrasburgo: En Diario Oficial de las Comunidades Europeas, L 194, 6 de julio de 2016. Recuperado el 10 de marzo de 2017, de http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L1148&from=ES

Poder Judicial de España. (s.f.). *El Plan de Modernización de la Justicia*. Recuperado el 6 de febrero de 2017, de http://www.poderjudicial.es/cgpj/es/Temas/Modernizacion-de-la-Justicia/El-Plan-de-Modernizacion-de-la-Justicia/

Poder Judicial de España. (s.f.). *Punto Neutro Judicial.* Recuperado el febrero de 13 de 2017, de http://www.poderjudicial.es/cgpj/es/Temas/e-Justicia/Servicios-informaticos/Punto-Neutro-Judicial/

Ponce Solé, J. (2001). *Deber de buena Administración y derecho al propio procedimiento administrativo debido. Las bases constitucionales del procedimiento administrativo y del ejercicio de la discrecionalidad.* Valladolid: Lex Nova.

Portal de Justicia de la Comunidad de Madrid. (s.f.). *Derechos y deberes de los ciudadanos ante la Administración de Justicia.* Recuperado el 20 de febrero de 2017, de http://www.madrid.org/cs/Satellite?cid=1354272665628&language=es&pageid=1354272673883&pagename=PJusticia%2FPJUS_Generico_FA%2FPJUS_fichaDetalle

Propiedad intelectual en la legislación colombiana. (s.f.). Recuperado el 25 de mayo de 2016, de El Derecho de Autor en la Era Digital: http://www.iered.org/miembros/ulises/representacion-ideas/Derechos-Autor/propiedad_intelectual_en_la_legislacin_colombiana.html

Protocolos y capas. (2017). *Técnicas de laboratorio.* Recuperado el 1 de junio de 2017, de http://www.eplc.umich.mx/salvadorgs/optativa/otros/capas.html

Ramelli, A. (2013). Seminario Internacional. Importancia de la construcción de contextos en las investigaciones judiciales. *Estructura de la Unidad Nacional de Análisis y Contextos (UNAC)* (págs. 76-82). Bogotá: Fiscalía General de la Nación. Unidad Nacional de Análisis y Contextos (UNAC). Recuperado el 20 de noviembre de 2016, de http://www.fiscalia.gov.co/colombia/wp-content/uploads/Seminario-Internacional-Construcci%C3%B3n-de-Contextos.pdf

Rayo, A. (2016). *Análisis de datos en big data: tipos y fases del análisis*. Recuperado el 3 de abril de 2017, de bit.es: Computer Training: http://www.bit.es/knowledge-center/analisis-de-datos-en-big-data/

Recuperación de Información en Internet. (2011). Recuperado el 30 de octubre de 2016, de http://sisinfo-sri.blogspot.com.co/2011/10/los-documentos-estructurados.html

Reed, M. (2013). Desafío en la construcción de contextos judiciales. *Seminario internacional. Importancia de la construcción de contextos en las investigaciones judiciales* (págs. 56-65). Bogotá: Fiscalía General de la Nación. Unidad de Análisis y Contextos (UNAC). Recuperado el 20 de noviembre de 2016, de http://www.fiscalia.gov.co/colombia/wp-content/uploads/Seminario-Internacional-Construcci%C3%B3n-de-Contextos.pdf

Romero-Morales, D., Smart, J., Shockley, R., Schroeck, M., & Tufano, P. (2012). *Analytics: el uso de big data en el mundo real.* En colaboración con la Escuela de Negocios Saïd en la Universidad de Oxford. Madrid: IBM España. IBM Corporation. Obtenido de http://www-05.ibm.com/services/es/gbs/consulting/pdf/El_uso_de_Big_Data_en_el_mundo_real.pdf

Russom, P. (2012). *Big Data Analytics, TDWI.* The Data Warehousing Institute.

Saiz, E. (13 de marzo de 2013). Los ciberataques sustituyen al terrorismo como primera amenaza para EE.UU. *El País*. Recuperado el 23 de noviembre de 2016, de https://elpais.com/internacional/2013/03/13/actualidad/1363187707_199021.html

Salvador, F. (2014). *Big data: ¿la ruta o el destino?* ie foundation y Oracle. Recuperado el 2 de junio de 2017, de https://bigdata299.files.wordpress.com/2015/11/big-data-esp-7.pdf

Sánchez Acevedo, M. E. (2015). El derecho a la buena Administración electrónica. Tesis doctoral. *Escola Tècnica Superior d'Enginyeria de la Universitat de València*, 276. Universidad de Valencia, España. Recuperado el agosto de 28 de 2017, de

http://roderic.uv.es/bitstream/handle/10550/50882/Tesis%20version%20final%20abierta.pdf?sequence=1&isAllowed=y

Taylor, S. J., & Bogdan, R. (1994). *Introducción a los métodos cualitativos de investigación.* Barcelona: Paidós.

Tomás Mallén, B. (2004). *El derecho fundamental a una buena Administración.* Madrid: INAP.

TRC Informática. (s.f.). *Conceptos básicos de big data.* Recuperado el 1° de junio de 2017, de http://www.trc.es/pdf/descargas/big_data.pdf

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), 207-246. (segunda etapa de la Revista "Autonomías"), monográfico sobre La incidencia de las TIC en el derecho público. Recuperado el 23 de noviembre de 2016, de https://dialnet.unirioja.es/servlet/articulo?codigo=2570101

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. (2013). Construcción de contextos y protección de las víctimas del conflicto armado. *Seminario internacional. Importancia de la construcción de contextos en la investigación judicial* (págs. 28-30). Bogotá: Fiscalía General de la Nación. Unidad de Análisis y Contextos (UNAC). Recuperado el 20 de noviembre de 2016, de http://www.fiscalia.gov.co/colombia/wp-content/uploads/Seminario-Internacional-Construcci%C3%B3n-de-Contextos.pdf

Villarubia C. DatacenterDynamics. (2014). Big data en la Policía Nacional. El cuerpo de seguridad implanta un proyecto de big data. *dcd.media*. Recuperado el 3 de noviembre de 2016, de https://www.dcd.media/videos/big-data-en-la-polic%C3%ADa-nacional-de-colombia/

Webster, J. (2012). *Examining HDFS and NameNode in Hadoop architecture*. Recuperado el 5 de febrero de 2017, de TechTarget: http://searchstorage.techtarget.com/video/Examining-HDFS-and-NameNode-in-Hadoop-architecture

Wills, M. (2013). Metodologías para la construcción de contextos históricos. *Seminario Internacional. Importancia de la construcción de contextos en las investigaciones judiciales* (págs. 47-52). Bogotá: Fiscalía General de la Nación. Unidad de Análisis y Contextos (UNAC). Recuperado el 20 de noviembre de 2016, de http://www.fiscalia.gov.co/colombia/wp-content/uploads/Seminario-Internacional-Construcci%C3%B3n-de-Contextos.pdf

Tablas y figuras

Tabla 2

Porcentaje de entidades del orden nacional que ofrecen servicios en línea, según tipo de actividad.

Actividad	%
Recibir respuestas a sus consultas vía correo electrónico o telefónicamente	87,0%
Hacer consultas vía correo electrónico	85,1%
Hacer denuncias, quejas y reclamos	84,4%
Descargar formularios (solamente)	60,4%
Completar/ registrarse en formularios en línea	53,9%
Servicios de salud	5,8%
Intermediación laboral	5,8%
Servicios de educación	5,2%
Descargar y enviar formularios	45,5%
Servicios de seguridad social	3,2%
Participación ciudadana (sistema de votación/elecciones, consultas públicas)	25,3%
Realizar pagos en línea (facturas, impuestos, salud, licencias, certificados)	24,0%
Capacitaciones virtuales	24,0%
Obtener certificados oficiales (a través de certificación o firma electrónica)	23,4%
Registro de empresas	12,3%
Hacer licitaciones	11,7%
Pagar impuestos	1,9%
Servicios de justicia	1,3%

Nota: Formulario único de reporte a la gestión. Fuente MinTic (2013).

Tabla 3

Construcción y análisis de indicadores de carga de trabajo de la FGN

Clasificación	Indicador	Ejemplo
Medición	Cuantitativos: Representación numérica de la realidad.	Porcentaje de entradas por delito (PED) $PED = \frac{Entradas\ del\ delito\ i}{Total\ de\ entradas}\ x100$
	Cualitativos: Calificación de una situación a partir de una escala de cualidades categóricas (alto, bajo, medio) o binarias (sí o no).	Percepción de seguridad en la ciudad: Percepción = (alta, media, baja)
Intervención	Resultado o producto: mide los logros obtenidos y la cantidad de bienes y servicios producidos por la ejecución de un proyecto, programa o política.	Tasa de condenas: $TI = \frac{Condenas}{Total\ entradas}\ x100$
	Proceso: mide el seguimiento a las actividades programadas.	Avance de la actividad x: Porcentaje de ejecución de la actividad X en el periodo *t* con respecto al periodo completo de ejecución
	Insumo: mide los recursos (humanos o materiales) disponibles para la ejecución de una actividad.	Fiscales por Dirección Seccional: Número de fiscales que componen una Dirección Seccional

Jerarquía	Estratégicos: miden la incidencia de los objetivos trazados hacia afuera de la organización.	Desarticulación de Bandas (DB): $DB = \left(\frac{NBD}{NTBI}\right) x100$ · NBD = Número de Bandas Desarticuladas · NTBI = Número Total de Bandas Identificadas
	Gestión: miden procesos operativos o administrativos de la organización.	Tasa de imputaciones (TI): $TI = \frac{Casos\ con\ Imp}{Total\ casos} x100$
Calidad	Eficacia: mide el logro de una meta.	Tasa de imputaciones (TI): $TI = \frac{Casos\ con\ Imp}{Total\ casos} x100$
	Eficiencia: relaciona los resultados obtenidos en función de los recursos invertidos para ello.	Productividad en la etapa de investigación (PI)[5]: $PI = \left(\frac{Formulación\ de\ Imp}{Fiscales}\right) x100$

Nota: Reelaborado a partir de la tabla de la Cartilla n° 4 (FGN, 2015b, pp. 8-9)

Tabla 4

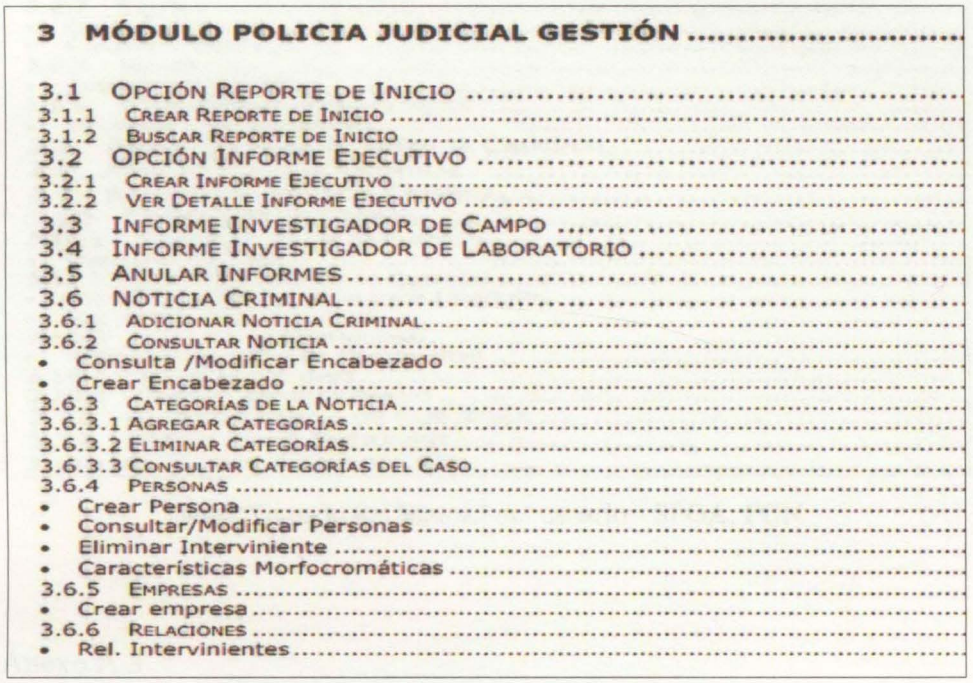
Construcción y análisis de indicadores de carga de trabajo de la FGN 2

Nombre del indicador[7]	Fórmula	Interpretación
Entradas efectivas (EF)	$EF = Entr - (ACA+AIH)$	¿Cuánto de lo que entró[8] efectivamente constituye un hecho delictivo sobre el cual la FGN debe responder? *ACA* = Archivos por Conducta Atípica. *AIH* = Archivos por Inexistencia del Hecho.
Tasa de imputaciones (TI)	$TI = \left(\frac{Imp}{EF}\right) x100$	¿Cuánto de lo que entró efectivamente se logró imputar?
Tasa de condenas (TC)	$TC = \left(\frac{Cond}{Imp}\right) x100$	¿Cuánto de lo que se imputó se logró condenar?
Tasa de escritos de acusación (TEA)	$TEA = \left(\frac{Esc\ Acu}{Imp}\right) x100$	¿Cuánto de lo que se imputó tiene escrito de acusación?
Tasa de archivos por imposibilidad de encontrar sujeto activo (TAI)	$TAI = \left(\frac{Arch\ Impos}{Entr}\right) x100$	¿Cuánto de lo que entró se archivó por imposibilidad de encontrar sujeto activo?
Tasa de evacuación (TE)	$TE = \left(\frac{Salidas}{Entr}\right) x100$	¿Cuánto salió[9] de lo que entró?
Carga de trabajo acumulada (CTA)	$CTA = EF - Salidas$	¿Cuánta carga de trabajo tengo acumulada?
Tasa de variación de la carga de trabajo (TVCT)	$TVCT = \left(\frac{CTA_t - CTA_{t-1}}{CTA_{t-1}}\right) x100$	¿Cuánto varió porcentualmente mi carga de trabajo acumulada de un periodo a otro?[10]
Índice de concentración de carga de trabajo por delito (ICCL)[11]	$ICCL_d = \sum_{h=1}^{H} \left(\frac{Entr_{dh}}{Entr_d}\right)^2$	¿Qué tan concentrada está la carga de trabajo en los despachos h por el delito *d*? $ICCL_d$ solo puede tomar valores entre 0 y 1, entre más se aleje de 0 hay mayor concentración[12].

Nota: Tomado de la Cartilla n° 4 (FGN, 2015b, p. 12)

Anexos

Anexo A 1



Nota: Tomado del Manual del usuario - SPOA, FGN

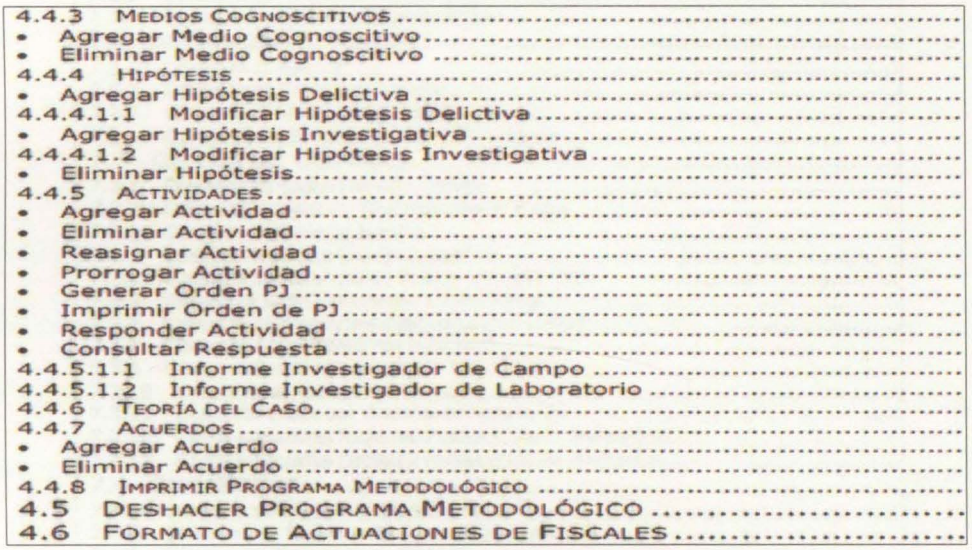
Anexo A 2

Nota: Tomado del Manual del usuario - SPOA, FGN

Anexo A 3

Nota: Tomado del Manual del usuario - SPOA, FGN

Anexo A 4



Nota: Tomado del Manual del usuario - SPOA, FGN

Anexo A 5

Nota: Tomado del Manual del usuario - SPOA, FGN

Glosario

Los siguientes términos, usados a lo largo de esta investigación, constituyen un conjunto de instrucciones expedidas por la FGN, cuya definición se presenta textualmente porque se deben comprender de acuerdo al significado que les da la entidad. Asimismo, se incluyen conceptos propios de la norma "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública [...]" (Congreso de la República, 2014, Ley 1712, epígrafe).

Actuación de Policía Judicial: actividades técnico-investigativas realizadas por la Policía Judicial que permiten verificar la ocurrencia de un hecho delictivo, determinar los presuntos autores y partícipes, así como aportar información y recolección de elementos materia de prueba o elementos materiales probatorios (en adelante: EMP) y evidencia física (en adelante: EF) útil para la actuación penal.

Análisis criminal: estudio sistemático e interdisciplinario del delito y de los factores problemáticos que alteran la convivencia social e interesan a la investigación penal (sociodemográficos, espaciales y temporales, entre otros), para apoyar la función constitucional asignada a la Fiscalía General de la Nación (en adelante: FGN) y propender por la garantía de los derechos fundamentales de las víctimas a la verdad, la justicia, la reparación y la no repetición.

Autoridad solicitante: se refiere a quienes por facultad legal pueden solicitar servicios a las direcciones, subdirecciones, departamentos, secciones, unidades y grupos de la FGN que cumplen actividades de Policía Judicial.

Análisis estratégico para la investigación criminal: estudio sistemático e interdisciplinario de fenómenos criminales de impacto criminal a partir de la identificación de planes y tendencias criminales a largo plazo. Consiste en analizar problemas delictuales o que tengan incidencia en la comisión de delitos, esto es, un conjunto de injustos penales que comparten ciertos factores comunes, imputables a organizaciones o redes delictivas que operan en determinada región o zona y que pueden ser responsables de la comisión de crímenes de manera masiva o sistemática.

Los análisis estratégicos se realizan para entender fenómenos de relevancia criminal de forma tal que produzcan insumos, que orienten y nutran la investigación penal, la toma de decisiones de altas instancias de la Fiscalía, la formulación de la política criminal, la generación de alertas tempranas y la generación de iniciativas investigativas. Este entendimiento puede ser delimitado por las variables modo, tiempo y lugar, entre otras.

Análisis operativo para la investigación criminal: uso de herramientas, técnicas y conocimientos específicos de forma tal que puedan orientar la investigación y suministrar resultados de corto plazo para el proceso investigativo de un caso o una situación delictiva particular. Dentro del análisis operativo se contemplan el análisis de caso, el análisis comparativo de casos, el análisis de grupo de autores, el análisis de la investigación, los análisis telefónicos, el análisis de relación de personas y organizaciones y el análisis de eventos, entre otros tipos de análisis que puedan ser pertinentes para la investigación criminal de acuerdo con la competencia y la especialidad.

Análisis para la investigación criminal: estudio sistemático que puede ser interdisciplinario de los factores problemáticos y delitos que se observan en fenómenos, situaciones y casos, a partir de la aplicación de diferentes técnicas y herramientas para optimizar el uso de la información, que respondan a las necesidades de la investigación criminal en la FGN.

Analista: servidor que está en capacidad de realizar funciones de análisis a partir del estudio disciplinado de los fenómenos criminales, los contextos y la estadística, en razón de su entrenamiento, conocimiento, experiencia investigativa, competencias o experiencia relacionada con metodologías de análisis y comprensión de los fenómenos criminales, etc.

Caso ilustrativo de plan criminal: situación fáctica representativa de los patrones de conducta delictiva característicos de determinada organización criminal.

Caso priorizado no imputable a una organización delictiva: conducta punible cuya realización no corresponde al accionar de una organización delictiva, pero que representa un elevado impacto social, tomando en consideración su gravedad, en términos de afectación de los derechos fundamentales de la víctima, de los bienes jurídicamente amparados o su capacidad para develar la existencia de patrones culturales discriminatorios.

Contexto: marco de referencia de aspectos esenciales acerca de elementos de orden geográfico, político, económico, histórico y social en el cual se han perpetrado delitos por parte de grupos criminales, incluidos aquellos con los cuales servidores públicos y particulares colaboran. Comprende una descripción de la estrategia de la organización delictiva, sus dinámicas regionales,

sus aspectos logísticos esenciales sus redes de comunicaciones, entre otros. La creación de contextos persigue: 1) conocer la verdad de lo sucedido; 2) evitar su repetición; 3) establecer la estructura de la organización delictiva; 4) determinar el grado de responsabilidad de los integrantes del grupo y de sus colaboradores; 5) unificar actuaciones dentro de la FGN con el fin de lograr esclarecer patrones de conducta, cadenas de mando fácticas; 6) emplear esquemas de doble imputación penal, entre otros aspectos.

Fuente formal: información que se recibe sobre la ocurrencia de hechos con característica de delito; se origina por 1) denuncia: la presenta cualquier persona natural o el representante legal de una persona jurídica afectada; 2) petición especial del Procurador General de la Nación, querella de la víctima o del directamente perjudicado, su representante legal o sus herederos, del defensor de familia o del agente del Ministerio Público, según el caso; 3) cualquier otro medio de origen oficial, como informes de Policía o de otra autoridad que haya tenido conocimiento de la ocurrencia de un hecho de probable connotación delictiva.

Fuente no formal: información de la que se pueda inferir una conducta punible, obtenida a través de informantes, escritos anónimos, llamadas telefónicas, las que provengan del espectro electromagnético y noticias difundidas a través de los medios de comunicación y las demás que lleguen a conocimiento de las autoridades.

Hipótesis: información o explicación tentativa que se pretende afirmar o refutar a partir de un estudio analítico y razonado. La hipótesis de trabajo en el proceso penal puede referirse a qué, quién, cómo, cuándo, dónde, por qué o para qué. En consecuencia, esta no se refiere únicamente a

la responsabilidad penal de una persona y es posible desarrollar varias hipótesis para explicar un mismo conjunto de datos.

Información: se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen; (2014, Ley 1712).

Información pública: es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal (2014, Ley 1712).

Información pública clasificada: es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley (2014, Ley 1712).

Información pública reservada: es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley (2014, Ley 1712).

Información exceptuada por daño a los intereses públicos: es toda aquella información pública reservada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito en las siguientes circunstancias, siempre que dicho acceso estuviere expresamente prohibido por

una norma legal o constitucional: a) La defensa y seguridad nacional; b) La seguridad pública; c) Las relaciones internacionales; d) La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso; e) El debido proceso y la igualdad de las partes en los procesos judiciales; f) La administración efectiva de la justicia; g) Los derechos de la infancia y la adolescencia; h) La estabilidad macroeconómica y financiera del país; i) La salud pública. (2014, Ley 1712, Art. 19)

Informes complementarios: informe de Policía Judicial emitido después del informe que cerró el acto urgente o descargó la orden de trabajo (OT), el cual ya ha sido entregado a la autoridad solicitante y que en control de calidad (producto no conforme) o por solicitud de autoridad destino se advierta una corrección, aclaración o adición anexo de información al informe inicial. Este informe no genera asignación de nueva OT, pero se debe registrar en el sistema de información y enviarlo a la autoridad mediante in oficio remisorio, en el cual se explica en qué numeral se cometió el error o se hace la aclaración o adición.

La copia del oficio remisorio y copia de informe de Policía Judicial hacen parte de la unidad documental inicial en el archivo de gestión. Este informe debe llevar el mismo número del informe al cual está dando alcance en la aclaración o corrección, adicionando un guion y el número correspondiente; por ejemplo 8754-1.

Informes de Policía Judicial: son los registros a través de los cuales los servidores de Policía Judicial presentan los resultados de las actividades investigativas, de campo y de laboratorio.

Informes parciales: informes de Policía Judicial que rinden los servidores para presentar resultados investigativos que requieren control legal o que, por su relevancia, la autoridad solicitante debe tener conocimiento de manera inmediata (consulta selectiva sobre bases de datos, vigilancias y seguimientos de personas o de cosas, interceptación de comunicaciones, análisis, entre otros). Con estos informes no se descarga la OT, sino la actuación de Policía Judicial realizada, y es responsabilidad del coordinador o jefe inmediato realizar el control respectivo. Cuando se presente el informe que cierra la OT, se deben relacionar en los anexos los informes parciales emitidos con su respectivo número, estar registrados en el sistema de información y hacer parte de la unidad documental que queda en el archivo de gestión.

Máximo responsable: este concepto se aplica en dos categorías diferentes: 1) aquel que dentro de la estructura de mando y control de la organización delictiva sabía o podía prever razonablemente la perpetración de crímenes en desarrollo de la ejecución de los planes operativos; y 2) de manera excepcional, se trata de aquellas personas que han cometido delitos particularmente notorios, con independencia de la posición que ocupaban en la organización delictiva.

Oficio petitorio: documento que aplica a los requerimientos previstos en la Ley 600 de 2000 asuntos penales y no penales generados por la autoridad solicitante.

Orden a Policía Judicial (OPJ): es el documento físico o electrónico en el cual el director de la investigación dispone de las actividades que debe desarrollar la Policía Judicial en cumplimiento del programa metodológico.

Orden de trabajo (OT): registro generado a través del sistema de información o cualquier otro medio, mediante asignación realizada por el subdirector, el jefe de departamento, sección o unidad o el coordinador de grupo, ante un requerimiento por parte de una autoridad solicitante.

Patrones criminales: conjunto de actividades, medios logísticos, de comunicación y modus operandi delictivo, desarrollados en un área y periodo determinados, de los cuales se pueden extraer conclusiones respecto a los diversos niveles de mando y control de la organización criminal.

Procedimiento de análisis para la investigación criminal: su objetivo principal es lograr una mayor efectividad en la investigación y judicialización de delitos complejos, a través de la comprensión interdisciplinaria de fenómenos, situaciones y casos que permitan orientar estrategias investigativas y focos de atención. Además, el procedimiento tiene los siguientes objetivos específicos: 1) estandarizar los parámetros del análisis de datos e información para la investigación criminal, de forma tal que permitan orientar la toma de decisiones tanto a nivel estratégico como operativo; 2) fortalecer las capacidades de análisis en todos los niveles de la FGN; 3) desarrollar herramientas interdisciplinarias para el análisis útiles a los servidores con funciones misionales, que permitan enfrentar fenómenos de criminalidad y generen mejores prácticas de investigación, dirigidas a orientar el proceso y la consecución de elementos probatorios útiles para la judicialización de casos y situaciones; 4) consolidar la labor de análisis y definir su alcance en el funcionamiento de la FGN.

Procedimiento del Sistema Penal Oral Acusatorio: su finalidad es estandarizar las actividades derivadas del SPOA con el fin de cumplir con la indagación, la investigación y el juicio de conformidad con la ley, así como las actividades de carácter administrativo que sirven de apoyo al proceso penal.

Procedimiento general para la Policía Judicial de la FGN: su objetivo es estandarizar los lineamientos relacionados con la recepción de la solicitud, asignación de OT, registro de actuaciones y resultados (sistemas de información y registros físicos), revisión del informe, descargue de la OT, envío del informe y archivo de la unidad documental.

Procedimiento Ley 600 de 2000: permite estandarizar las actividades derivadas del proceso penal bajo la Ley 600 de 2000, con el fin de optimizar la gestión en la investigación, acusación y juicio, así como las actividades de carácter administrativo que surgen en desarrollo del proceso penal.

Procedimiento para aplicación del sistema de responsabilidad penal para adolescentes: está encaminado a estandarizar las actividades para la aplicación de la Ley 1098 de 2006 y demás normas concordantes que rijan el Sistema de Responsabilidad Penal para Adolescentes (SRPA), por parte de la FGN.

Programa metodológico: mesa de trabajo entre el fiscal, como director de la investigación, y los integrantes de Policía Judicial, donde se determinan los objetivos relacionados con la naturaleza de la hipótesis delictiva, los criterios para evaluar la información obtenida, la delimitación funcional de las tareas que se deben adelantar en procura de los objetivos trazados, el

procedimiento de control en el desarrollo de las labores realizadas y el seguimiento a lo obtenido para que se logren resultados acordes con la investigación. El fiscal ordenará la realización de todas las actividades que no impliquen restricción a los derechos fundamentales y que sean conducentes al esclarecimiento de los hechos, al descubrimiento de los elementos materiales probatorios y evidencia física, a la individualización de los autores y partícipes del delito, a la evaluación y cuantificación de los daños causados y a la asistencia y protección de las víctimas (artículo 207 CPP).

Reporte de inicio (FPJ-01): aviso que hace la Policía Judicial al fiscal acerca de la posible ocurrencia de un hecho punible, para que asuma la dirección, coordinación y control de la investigación.

SIJYP: sistema de información para funcionarios y servidores de la FGN que tiene por objetivo registrar todas las actuaciones de investigación de los procesos que se siguen en el marco de la Ley 975/2005 de Justicia y Paz. Este sistema de información cuenta con registros e informaciones que no se cruzan con los sistemas de información SPOA y SIJUF.

SIJUF: sistema de información para funcionarios y servidores de la FGN que tiene por objetivo registrar todas las actuaciones de investigación de los procesos que se siguen en el marco de la Ley 600 de 2000. Este sistema de información cuenta con registros e informaciones que no se cruzan con los sistemas de información: SPOA y SIJYP.

Solicitud de análisis de EMP o EF (FPJ-12): petición que se origina dentro de una investigación, ya sea por actos urgentes o por OPJ para realizar un estudio o análisis de EMP y EF.

Solicitud de apoyo investigativo: es el mecanismo que debe utilizar un investigador de Policía Judicial de la Fiscalía General de la Nación cuando requiere el apoyo de otro investigador para la ejecución de actuaciones de Policía Judicial, cuando dichas actividades son en jurisdicción distante a la suya, con el fin de evitar el desplazamiento del investigador y mejorar la oportunidad en la respuesta a la autoridad.

Solicitud verbal: en aplicación a la Ley 906 de 2004 y en los casos que sean pertinentes, se atenderán dichas solicitudes y se deben materializar antes de la entrega del informe en solicitud de análisis de EMP y EF (FPJ-12), OPJ u oficio.

SPOA: es el sistema de información que registra las actividades de investigación seguidas por el procedimiento general de investigación de la Ley 906 de 2004; este no se cruza con informaciones registradas en los sistemas de información de Ley 600 de 200 ni los de la Ley 975 de 2005.