Ciberseguridad en la justicia digital, recomendaciones para el caso colombiano

Maribel Patricia Rodríguez Márquez
Jenny Marcela Sánchez Torres

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

2020

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL FUERZAS MILITARES
ESCUELA SUPERIOR DE GUERRA

CIBERSEGURIDAD EN LA JUSTICIA DIGITAL, RECOMENDACIONES PARA EL CASO COLOMBIANO.

UNA REVISIÓN DE LITERATURA

ALUMNA:

MARIBEL PATRICIA RODRÍGUEZ MÁRQUEZ

TUTORA:

JENNY MARCELA SÁNCHEZ-TORRES, Ph.D

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO – ARTÍCULO DE INVESTIGACIÓN

BOGOTA – COLOMBIA

2020

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL FUERZAS MILITARES
ESCUELA SUPERIOR DE GUERRA
MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

CIBERSEGURIDAD EN LA JUSTICIA DIGITAL, RECOMENDACIONES PARA EL CASO COLOMBIANO.

UNA REVISIÓN DE LITERATURA

ALUMNA: MARIBEL PATRICIA RODRÍGUEZ MÁRQUEZ

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO – ARTÍCULO DE INVESTIGACIÓN PARA OPTAR EL TITULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA

BOGOTA – COLOMBIA

2020

Declaración de originalidad por parte del autor

Mediante la presente certifico que soy la única autora de este artículo de investigación. Todos los materiales usados, referencias de literatura y estudios elaborados por otras personas han sido referenciados en el presente documento. El artículo fue sustentado el 08 de septiembre de 2020 con la aprobación, ha sido sometido para publicación en la revista UIS ingenierías.

Autor: MARIBEL PATRICIA RODRÍGUEZ MÁRQUEZ

Noviembre, 2020

Agradecimientos

A Dios por haberme dado esta oportunidad de crecimiento profesional y personal, y en quien me refugié en los días que no me sentía con fuerzas para seguir adelante.

A mi madre por sembrar en mi los principios y valores, la honestidad, la tenacidad y la perseverancia para alcanzar los sueños que nos proponemos.

A mi hija por su paciencia y amor.

A mi familia quienes, con su amor y apoyo en medio de las circunstancias me alentaron con sus oraciones.

A Julián, quien me motivó a participar de esta beca de estudio y siempre ha estado ahí para mí.

A mi Directora del presente trabajo de grado, la Doctora Jenny Marcela Sánchez-Torres, principal colaboradora durante todo este proceso, quien con su dirección, conocimiento, enseñanza, colaboración, paciencia, sabiduría y apoyo incondicional permitió el desarrollo de este trabajo de investigación. A ella muchas gracias por toda su dedicación.

A los jurados Profesores Jairo Becerra, Marcos Sánchez Acevedo, Capitan Gladys Medina por los comentarios dados antes y durante el proceso de sustentación, igualmente, a los revisores del artículo sometido a la revista UIS Ingenierías, todos ellos permitieron enriquecer el texto del artículo.

Finalmente expresar mi agradecimiento al Ministerio de Tecnologías de la Información y las Comunicaciones, a la Escuela Superior de Guerra "General Rafael Reyes Prieto"– Ministerio de Defensa por la beca otorgada por el programa de formación en la Maestría en Ciberseguridad y Ciberdefensa.

Resumen

Ciberseguridad en la justicia digital, recomendaciones para el caso colombiano. Una revisión de literatura.

La adopción de las Tecnologías de la Información y las Comunicaciones -TIC- ha causado tanto al sector público como al privado múltiples transformaciones. El uso de las TIC en el sector justicia agiliza los procesos judiciales. Sin embargo, ese uso también constituye un riesgo, por cuanto la justicia es parte de la infraestructura crítica de las naciones, aunado a las características de la información que atañe a los procesos, una interrupción de la prestación de esos servicios sería catastrófica. Por tal razón, la ciberseguridad juega un papel en cada una de las etapas de los procesos judiciales digitales. En ese sentido el objetivo de este artículo de revisión es proponer recomendaciones en ciberseguridad aplicables a los procesos judiciales digitales en el caso colombiano a partir de una revisión sistemática de literatura, que permitió analizar el panorama de la justicia digital con énfasis en Latinoamérica, las TIC que suelen usarse en cada una de las etapas del proceso judicial digital, los riesgos cibernéticos, las recomendaciones para enfrentarlos, y cómo las funciones del marco de ciberseguridad de la *National Institute of Standards and Technology* –NIST- son consideradas.

Palabras claves: **justicia digital; ciberseguridad; procesos judiciales digitales.**

Abstract

Cybersecurity in digital justice, clues for Colombian case. A literatura review

The adoption of Information and Communication Technologies -ICT- has caused multiple transformations both public and private sectors. The use of ICT in the justice sector speeds up judicial processes. However, this use raises risks, since justice is part of the critical infrastructure of nations, next to judicial information's characteristics, an interruption in the provision of these services would be catastrophic. For this reason, cybersecurity plays a role in each stage of digital judicial processes. This paper aims to propose cybersecurity recommendations to digital judicial processes in the Colombian case based on literature analysis, which described the digital justice landscape with an emphasis on Latin America. It also analyzes which ICT are used in each stage of the digital judicial process, their cyber risks, and the recommendations to face them, and how the functions of the de la National Institute of Standards and Technology –NIST- cybersecurity framework are considered.

Keywords**: digital justice, cybersecurity, digital judicial processes.**

Tabla de abreviaciones y términos

NIST	Instituto Nacional de Estándares y Tecnología
TIC	Tecnologías de la Información y las Comunicaciones

Tabla de contenido

Listas de Tablas

Lista de Figuras

Ciberseguridad en la justicia digital, recomendaciones para el caso colombiano. Una revisión de literatura.

Cybersecurity in digital justice, clues for Colombian case. A literatura review.

Maribel Patricia Rodríguez-Márquez [1],

[1] El presente artículo de investigación es presentado como opción de grado para optar al título de Magister en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra, siendo producto del proyecto de investigación aprobado por el comité de investigación vinculado al grupo de investigación respectivo inscrito en MinCiencias. correo electrónico: maribelp.rodriguez@esdegue.edu.co

1. Introducción

Desde finales del siglo pasado, el uso de las Tecnologías de la Información y las Comunicaciones -TIC- en diferentes ámbitos ha causado una transformación en las formas de desarrollo de cada uno de tales ámbitos (Castells, 1996; Sánchez-Torres, González-Zabala, & Sánchez-Muñoz, 2012).

El sector justicia no es la excepción. El uso de las TIC en el sector justicia, o justicia digital, va desde el uso de archivos electrónicos hasta las videoconferencias para las audiencias en los juicios, entre otros.

La justicia es un servicio público básico e imprescindible, es esencial y hace parte del Estado de derecho. Si se interrumpiera la prestación de Justicia se causaría a la población un altísimo perjuicio, por ello hace parte de la infraestructura crítica (Klaver, Luiijf, Nieuwenhuijs, & Al, 2011). En ese sentido, si bien la justicia digital implica beneficios, también hay algunos riesgos. Entre los beneficios están la eficiencia, la transparencia, la reducción de costos y de tiempos (Cerrillo i Martínez, 2007; Herbert, 2015).

Sin embargo, derivado de la información sensible que el sistema judicial maneja, se constituye en un atractivo para los cibercriminales, hackctivistas entre otros, si la información judicial cae en esas manos criminales ello que puede llegar a ser muy lesivo para los diferentes usuarios de la administración de justicia (Gordon & Garrie, 2020). Pese a ello, es poca la literatura que examina las consecuencias de la incorporación de las TIC en los procedimientos de la administración de justicia (Donoghue, 2017) y más escasa la literatura relacionada con la ciberseguridad en la justicia digital.

Ahora bien, Colombia, desde hace varias décadas, tiene una crisis judicial profunda que no permite que el sistema judicial satisfaga las demandas de la población, por ello se han implementado varios planes de descongestión, y esfuerzos de modernización tecnológica y transformación digital para fortalecer y mejorar el servicio de justicia en el país, a través del impulso del uso de las TIC y de herramientas disruptivas como la analítica de datos y la inteligencia artificial, apoyada en una política de seguridad de la información y protección de datos (Consejo Superior de la Judicatura, 2017, 2019; Ministerio de las Tecnologías de la información y comunicaciones de Colombia, 2008).

La incursión de estas tecnologías, y el atractivo de la información judicial por parte de los cibercriminales propicia el objetivo de este artículo que es proponer recomendaciones en ciberseguridad aplicables a los procesos judiciales digitales en el caso colombiano a partir de una revisión sistemática de literatura que analizó cuál es el panorama de la justicia digital, cuáles son las TIC que suelen usarse en cada una de las etapas del proceso judicial digital, cuáles son los riesgos cibernéticos y recomendaciones para enfrentarlos, cómo las funciones del marco de ciberseguridad de la NIST son consideradas en las etapas de los procesos judiciales digitales.

Este artículo está estructurado en seis secciones, la segunda describe el contexto de la justicia digital, de la ciberseguridad y del marco de ciberseguridad NIST. La tercera sección describe el método de revisión sistemática de literatura empleado. La cuarta presenta y discute los resultados; la quinta presenta las recomendaciones que podrían aplicarse al caso

colombiano; y la sexta presenta las conclusiones y sugerencias para futuros estudios.

2. Marco Conceptual y contexto

A continuación, se exponen los elementos conceptuales necesarios para el desarrollo de esta investigación.

2.1. Justicia digital

Desde los años 90 son varias las iniciativas de la incorporación de las TIC en la administración de justicia (Rosa, Teixeira, & Sousa Pinto, 2013; Sánchez-Torres, 1998). La justicia digital, hace parte del gobierno electrónico[2], entendido como el uso de las TIC para el desarrollo de una administración pública eficiente, en la prestación de servicios e información a los ciudadanos y empresas (Heeks, 2005; Katz & Hilbert, 2003; Sánchez-Torres, 2005).

La justicia digital constituye un sector de la Sociedad de la Información[3]. Una definición amplia de la justicia digital contempla el uso de las TIC para prevenir el crimen, mejorar la administración de justicia y el sistema legislativo (Aaltonen, Laarni, & Tammela, 2015; Velicogna, 2017). La justicia digital busca mejorar el acceso de los ciudadanos a la justicia

[2] El concepto de gobierno electrónico fue propuesto en 1997 por el gobierno de Estados Unidos. El gobierno electrónico es también conocido como gobierno digital, gobierno en línea, *e-government* entre otros

[3] Desde hace ya varias décadas, es reconocido que la clave del desarrollo económico y social pasa por la adopción y uso de las TIC en diversos sectores productivos. Así autores como Masuda y Konichi en 1968, Bell en los años 70, Castells en los 90, a éste fenómeno le han llamado Sociedad de la Información y consideran que surge como una respuesta evolutiva a la sociedad industrial y post industrial de los siglos XIX y XX (Castells, 1996; Sánchez-Torres et al., 2012). (Hilbert, 2012) modela la sociedad de la información como un cubo tridimensional compuesto por tres estratos: un primer estrato vertical conformado por los sectores en los cuales se divide la sociedad de la información como lo son el sector e-gobierno, e-salud, e-educación, entre otros; un segundo estrato que involucra aspectos transversales como la regulación, la legislación en incentivos y el financiamiento; y un tercer estrato horizontal compuesto por la infraestructura, los servicios genéricos y las capacidades y habilidades para diseñar y usar esos servicios.

y a la acción judicial efectiva, que consiste en la solución de controversias o la imposición de sanciones penales. La justicia digital también es conocida como justicia electrónica, e-justicia, justicia on-line o ciberjusticia.

Los objetivos específicos de la justicia electrónica son: economía y concentración procesal; evitar el rezago de expedientes (para hacer más eficiente la impartición de la justicia); incrementar la transparencia; incrementar el acceso a los servicios de justicia; acercar a los ciudadanos y propender por su participación; y reducir los costos de los procesos judiciales (Canivet, 2016; Cerrillo i Martínez, 2007; García Barrera, 2018; Weinstock, 2016).

La justicia digital involucra, desde los métodos de comunicación como el correo electrónico, las videoconferencias, los sistemas de resolución de conflictos en línea, hasta los sistemas de información para la gestión de los procesos pasando por las tecnologías para los tribunales (salas de audiencia), los servicios en línea para consulta de los ciudadanos, entre otros (Contini & Velicogna, 2011; Londoño-Sepulveda, 2010; Velicogna, 2017).

La Justicia digital, además, implica el desarrollo del marco regulatorio necesario para habilitar su uso que faciliten sustituir los elementos analógicos por los digitales, la coordinación del capital humano, los medios financieros y auxiliarse de todos los medios tecnológicos que ayuden a ser más eficiente la administración de justicia (Álvarez- Casallas, 2010).

Son varios los beneficios de incorporar las TIC en la administración de justicia: un sistema judicial más eficiente gracias a la reducción de los costos de transacción; un sistema judicial efectivo gracias a la reducción de la duración de los procesos, que implica ahorros de tiempo, dinero y trabajo; la administración de justicia puede ofrecer mayor información y

transparencia sobre su funcionamiento; facilitar el acceso a la justicia por parte de los ciudadanos, en especial determinados colectivos tales como: los inmigrantes, personas con bajo nivel cultural, discapacitados, entre otros (Al Swelmiyeen & Al-Nuemat, 2017; Cerrillo i Martínez, 2007; Comisión Europea, 2010; Pontificia Universidad Javeriana et al., 2019; Weinstock, 2016).

Algunos autores consideran que el uso de las TIC en el sistema judicial puede darse en los siguientes ámbitos: i) como apoyo a la gestión del proceso, es decir facilitar el almacenamiento y búsqueda con agilidad tanto de la información jurídica como de todos y cada uno de los documentos soporte como fallos, sentencias, resoluciones, entre otros y de las evidencias; ii) en la fase decisoria, en la que las TIC son un soporte para que los jueces puedan tomar sus decisiones (Álvarez-Casallas, 2010; García Barrera, 2018).

En línea con los ámbitos señalados, en el caso colombiano y siguiendo las pautas expresadas en el Código General del Proceso Ley 1564 de 2012 (Congreso de la República de Colombia, 2012) el cual regula la actividad procesal en asuntos civiles, de familia, agrarios y comerciales, y de otras jurisdicciones cuando en estas surjan vacíos siempre que no riña con sus principios rectores, un proceso judicial de manera general está constituido por las siguientes etapas: Presentación de la demanda, admisión, inadmisión y/o rechazo de la demanda; Contestación de la demanda, audiencias y diligencias; Decreto y práctica de Pruebas; Alegatos, Sentencia. Por su parte, en el Código de Procedimiento Penal Ley 906 de 2004 un proceso judicial en general, comprende las siguientes grandes etapas: noticia criminal, denuncia, indagación e investigación, y ejecución de sentencia.

A partir de lo anterior, para esta investigación las grandes etapas de un proceso judicial son: (i) Gestión del proceso judicial, que comprenderá aspectos como la recepción de la demanda entendida como la solicitud de inicio de un proceso judicial ante autoridad jurisdiccional competente; también implica las audiencias y diligencias que corresponde a las que se realizan dentro de un proceso, en la cual la autoridad judicial oye a los sujetos procesales; (ii) Pruebas o evidencias se refieren a los elementos de convicción aportados dentro de un proceso judicial; (iii) Sentencia corresponde a la decisión de la autoridad judicial basada en su criterio y en derecho; y, (iv) Ejecución de sentencia entendida como la ejecución de la sanción penal o civil impuesta mediante sentencia ejecutoriada.

2.2. Ciberseguridad

En la literatura se encuentran varias definiciones de Ciberseguridad, sin embargo, entre las más conocidas se destacan:

i) La Unión Internacional de Telecomunicaciones -UIT- la define como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Las propiedades de seguridad incluyen uno o más de las siguientes: disponibilidad, integridad (que puede incluir autenticidad y el no repudio) y confidencialidad (UIT, 2008);

ii) Conforme a la norma ISO/IEC 27032:2012 señala que la ciberseguridad se trata de la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, definiendo a su vez ciberespacio como el entorno complejo resultante de la

interacción de personas, software y servicios en Internet, a través de dispositivos tecnológicos y redes conectadas a él, que no existen en ninguna forma física (The International Organization for Standardization, 2012);

iii) Según la Agencia Europea para la seguridad de la información y las redes, el ciberespacio es el conjunto de activos tangibles e intangibles que dependen del tiempo y que almacenan y transfieren información electrónica. Además, la agencia señala que la ciberseguridad comprende todas las actividades necesarias para proteger el ciberespacio,sus usuarios y las personas afectadas de las amenazas cibernéticas, es decir, la ciberseguridad abarca todos los aspectos de prevención, previsión, tolerancia, detección, mitigación, eliminación, análisis e investigación de incidentes cibernéticos. Teniendo en cuenta los diferentes tipos de componentes del ciberespacio, la ciberseguridad debe cubrir los siguientes atributos: disponibilidad, confiabilidad, seguridad, confidencialidad, integridad, mantenibilidad (para sistemas tangibles, información y redes), robustez, supervivencia, resistencia (para apoyar la dinámica del ciberespacio), responsabilidad, autenticidad y no repudio (para apoyar la seguridad de la información (European Union Agency for Network and Information Security, 2017);

iv) Para el gobierno colombiano, en documento del Consejo Nacional de Política Económica y Social -CONPES- 3854 de 2016, la ciberseguridad es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio (Departamento Nacional de

Planeación, 2016). En el documento del CONPES 3995 de 2020, reitera la definición enmarcada en el anterior documento CONPES la cual se entiende como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética, buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio de las interacciones digitales (Departamento Nacional de Planeación, 2020).

2.3. Marco de Ciberseguridad - NIST

Un marco de ciberseguridad es un conjunto de estándares, directrices y mejores prácticas para gestionar los riesgos relacionados con la ciberseguridad. Son varios los que han sido reconocidos y adoptados con mayor frecuencia, a saber: los estándares ISO/IEC 27001/27002; seguido del estándar PCI DSS (Payment Card Industry Data Security Standard); CIS Critical Security Controls; las diferentes versiones de la Guía Estratégica Nacional de Ciberseguridad de la UIT y el marco para la Ciberseguridad NIST.

El marco para la Ciberseguridad NIST, cuya primera versión se lanzó en 2014, y se actualizó en 2018, su estructura se basó en el marco CIS, COBIT y la ISO/IEC 27001, se caracteriza por considerar la Ciberseguridad como un ciclo de proceso evolutivo que permite obtener una mejora continua en las organizaciones alrededor del tema de Ciberseguridad. Según el estudio de (Dimensional Research, 2016), 300 profesionales de seguridad en TI de los Estados Unidos, señaló que el 70% de ellos considera el marco de ciberseguridad NIST como una buena práctica.

El marco de ciberseguridad NIST consta de cinco funciones, con 23 categorías y 108 subcategorías. Las cinco funciones de alto nivel, que apoyan a las organizaciones en la toma

de decisiones frente a la gestión del riesgo son (National Institute of Standards and Technology, 2018):

i) Identificar: permite determinar los sistemas, activos, datos y competencias de la organización, su contexto de negocio, los recursos que soportan las funciones críticas y los riesgos de ciberseguridad que afectan este entorno;

ii) Proteger: permite desarrollar e implementar las contramedidas y salvaguardas necesarias para limitar o contener el impacto de un evento potencial de ciberseguridad;

iii) Detectar: permite el descubrimiento oportuno de la ocurrencia, realizan una vez detectado un incidente de ciberseguridad y tener la capacidad de contenerlo;

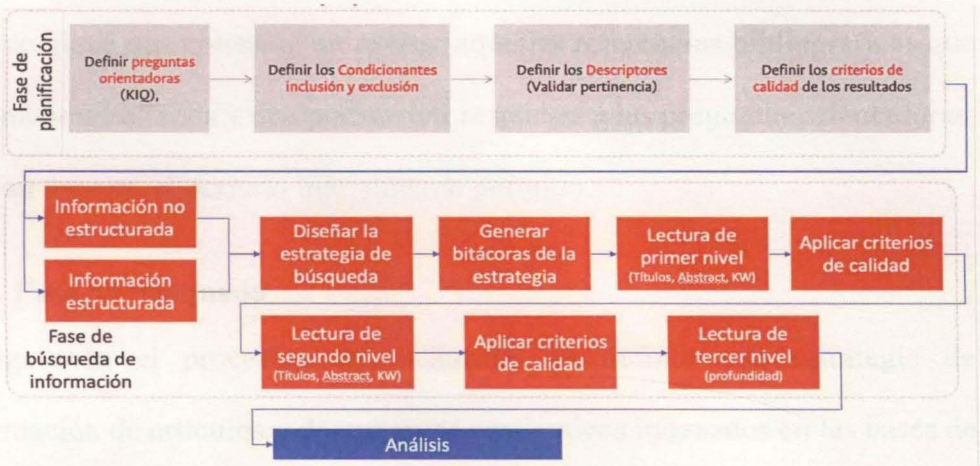
iv) Responder: Permite la definición y despliegue de actividades para reaccionar frente a un evento de ciberseguridad identificado y mitigar su impacto;

v) Recuperar: permite el despliegue de actividades para la gestión de resiliencia y el retorno a la operación normal después de un incidente.

3. Método

Con el fin de dar respuesta a la pregunta de investigación, se realizó una revisión Sistemática de Literatura siguiendo el procedimiento propuesto por Sánchez-Torres, (2017) quien amplia el procedimiento propuesto por Kitchenham et al., (2009). Dicho procedimiento, conforme se observa en la Figura 1 propone tres fases, a saber: i) planificación; ii) búsqueda de información; y, iii) análisis.

Figura 1 Esquema del método



Fuente: Sánchez-Torres, (2017)

3.1.Fase de Planificación

En la etapa de planificación se definieron las siguientes preguntas orientadoras:

PO1: ¿Porqué es importante considerar la ciberseguridad en la justicia digital?

PO2: ¿Cuál es el panorama de las iniciativas de justicia digital con especial énfasis en Latinoamérica?

PO3: ¿Cuáles son las TIC que se usan, los riesgos cibernéticos y las recomendaciones para cada una de las diferentes etapas de un proceso judicial?

PO4: ¿Cuáles son las funciones y subcategorías del marco de ciberseguridad NIST de manera general y a la luz de las etapas de un proceso judicial?

Como criterios de inclusión se tuvo en cuenta la fecha de publicación del documento, pues se tuvieron en cuenta aquellos publicados en el periodo comprendido entre el año 2015 y el 2020; que diese indicios para responder las preguntas orientadoras. El idioma de las publicaciones podría ser inglés, castellano, portugués, italiano y francés. Se definieron como

criterios de calidad que el documento diese respuesta al objetivo que pretendía alcanzar y describiese con claridad el método con que fue elaborado. También se utilizó la estrategia de bola de nieve que consistió en revisar aquellas referencias bibliográficas que se citan en los documentos hallados y que podrán dar respuesta a las preguntas orientadoras, sin importar si estaban o no en el periodo inicialmente definido.

3.2. Fase de búsqueda

Siguiendo el procedimiento señalado, se definió una estrategia de búsqueda de información de artículos y documentos académicos indexados en las bases de datos: JSTOR, Scopus, ACM y Scielo. También se definió otra estrategia de búsqueda de información no estructurada en castellano.

En este sentido, se realizaron diferentes iteraciones para mejorar las estrategias de búsqueda y obtener documentos que puedan dar respuesta a las preguntas orientadoras. Una vez aplicadas las estrategias de búsqueda, para las bases de datos mencionadas se obtuvieron un total de 1098 documentos. Posteriormente, al aplicar los criterios de inclusión y exclusión en la lectura de los abstracts y títulos se seleccionaron un total de 93 documentos para su lectura en profundidad. También se utilizó la estrategia de bola de nieve que consistió en revisar aquellas referencias bibliográficas que se citan en los documentos hallados y que podrán dar respuesta a las preguntas orientadoras, sin importar si estaban o no en el periodo inicialmente definido.

En la Tabla 1 se discrimina la estrategia de búsqueda, la base de datos, y el número de documentos obtenidos y analizados.

Tabla 1 Estrategias de búsqueda

Tipo de Fuente	Base de datos / motor	Estrategia de búsqueda	Número de documentos	
			iniciales	analizar
Información estructurada -	JSTOR	((*cybersecurity OR "cyber security") AND (justice OR "judicial system" OR "criminal justice" OR cyberjustice OR "judicial process" OR e-justice OR "digital justice")*) AND Pubyear >= 2015	795	36
	ACM		171	15
	Scopus		94	28
	Scielo	Justicia electrónica	18	2
Información no estructurada	Google	Ciberseguridad .AND. "justicia electrónica" filetype:pdf	20	12

Fuente: Elaboración propia

3.3. Fase de Análisis de los hallazgos obtenidos

Siguiendo el método reseñado, 110 documentos fueron leídos en profundidad y se clasificaron según las etapas de un proceso judicial y las funciones y subcategorías de la NIST, antes mencionadas. La clasificación se registró en el campo de palabras claves del software bibliográfico Mendeley. Posteriormente, utilizando el software VoSViewer, se realizó un análisis de co-ocurrencia de las palabras claves de los documentos seleccionados las cuales fueron traducidas al castellano, que junto con la clasificación previamente realizada facilitó ver las relaciones en los documentos. En la sección de resultados se presentan las respuestas a las preguntas orientadoras y los hallazgos de tales análisis.

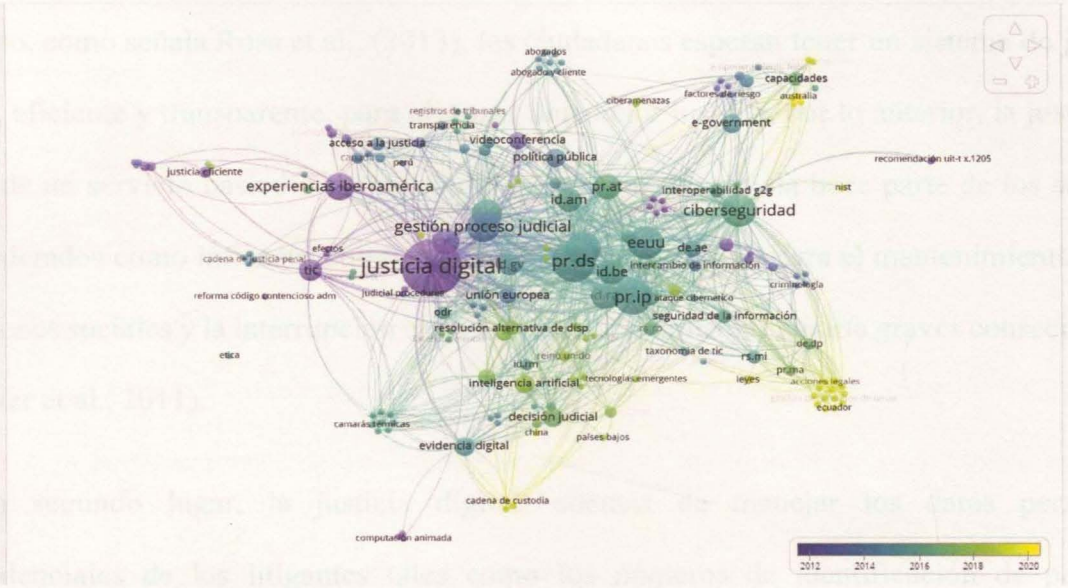
4. Resultados

4.1. Descripción general de los documentos

El conjunto de 110 documentos estaba conformado por 36 artículos de revista, 23 informes, 5 libros, 19 capítulos de libros, 12 artículos presentados en conferencias, 9 normas o leyes, 6 tesis. En cuanto al origen geográfico de aquellos documentos que describen casos se encontró que 55 se desarrollan en América (24 de Estados Unidos, 25 están relacionados

con Latinoamérica -Argentina, Brasil, Colombia, Costa Rica, El Salvador, México, Perú, Venezuela- y seis son de Canadá); 12 son de Europa (Francia, Finlandia, Holanda, Noruega, Reino Unido) y cinco son de Asia (China, India, Jordania, Malasia) y uno de África (Cabo Verde).

Figura 2 Análisis de co-ocurrencia de palabras y su agrupación en el tiempo



Fuente: Elaboración propia usando el software VoSViewer.

El análisis de co-ocurrencia de palabras clave presentado en la Figura 2 muestra tres conjuntos de documentos a lo largo del tiempo: i) un primer conjunto con documentos donde se presentan las bases conceptuales de la justicia digital identificados en color morado, documentos fechados entre 1995 y el 2013; otro conjunto de documentos donde se habla de los riesgos cibernéticos, y las funciones asociadas al marco de ciberseguridad NIST identificados con color verde, publicados entre 2014 y 2018 y, un último conjunto de documentos, en color amarillo, donde se presentan técnicas computacionales disruptivas como la inteligencia artificial publicados entre 2019 y lo que va corrido de 2020.

4.2.Importancia de la ciberseguridad en la justicia digital

De acuerdo con los hallazgos de la RSL son varias las razones para considerar la ciberseguridad en la justicia digital:

En primer lugar, es importante tener presente que la separación entre los poderes ejecutivos, legislativos y judiciales es la piedra angular de los países democráticos. En ese sentido, como señala Rosa et al., (2013), los ciudadanos esperan tener un sistema de justicia justo, eficiente y transparente, para alcanzar una mejor justicia, por lo anterior, la justicia se trata de un servicio básico e imprescindible. Por ello, la justicia hace parte de los sectores considerados como infraestructuras críticas que son esenciales para el mantenimiento de las funciones sociales y la interrupción o destrucción de las mismas tendría graves consecuencias (Klaver et al., 2011).

En segundo lugar, la justicia digital, además de manejar los datos personales confidenciales de los litigantes tales como los números de identificación de personas naturales y jurídicas, números de cuentas bancarias, información de la víctima en casos de violencia doméstica y agresión sexual, archivos de la jurisdicción de familia que involucran a niños y familias; informes médicos y psicológicos; testimonios dentro de transcripciones y grabaciones selladas; propiedad intelectual y secretos comerciales; registros de deliberación judicial; datos de los servidores judiciales, datos financieros del sistema judicial, entre otros que se constituyen en información sensible, puede contener información confidencial del gobierno relacionada con la seguridad nacional. Por ello, se requiere que el umbral de protección de datos sea mucho más alto y se refuerza el concepto de infraestructura crítica

(Benyekhlef, 2018; Mclaughlin, 2018; Palmgren, 2018).

En tercer lugar, cuando la prestación del servicio de justicia se realiza mediado por las TIC, pese a la especificidad del sistema judicial, no es muy diferente del uso de las TIC por parte de las instituciones financieras, las empresas, las Pymes, u otras entidades estatales. Sin embargo, por su responsabilidad pública, convierte al sistema judicial en un objetivo para los cibercriminales (Mclaughlin, 2018), como lo señalan Ganesin, Supayah, & Jamaludi, (2016) y Pijnenburg-Muller, (2015) la ciberseguridad debe ser contemplada en todas las áreas de la sociedad: la judicial, la social y la económica en especial para los países en desarrollo.

Y, en último lugar, los datos judiciales son valiosos para los ciberdelincuentes por varias razones. Primero, esta información podría ser utilizada para propósitos criminales. Segundo, los criminales pueden querer secuestrar este tipo de datos y pedir por el pago del rescate [4]. El costo de la pérdida o robo de información sensible es un serio problema (Norris Rodin & Rodin, 2015). Tercero, el acceso a los sistemas judiciales podría permitir a los ciberdelincuentes manipular los registros de datos judiciales, poniendo en peligro la credibilidad del proceso judicial. Cuarto, los registros confidenciales podrían usarse como parte de una estrategia legal en una gran cantidad de tipos de expedientes. Finalmente, las violaciones de la privacidad de los datos pueden detener las operaciones judiciales a medida que se ejecutan las medidas de respuesta (Mclaughlin, 2018).

[4] Como ocurrió, en el Tribunal de Menores del Condado de Columbia y la Oficina del Secretario del circuito en Ohio, así como en la Rama Judicial en Minnesota, en Estados Unidos en 2017 (Mclaughlin, 2018).

4.3. Panorama de las iniciativas de justicia digital, con especial énfasis en Latinoamérica.

Como lo señala Aspis (2010), la utilización de las TIC reduce la burocratización que enferma los procesos de los tribunales, tanto latinoamericanos como europeos. Por ello, el desarrollo de la justicia digital es considerada un elemento clave en la modernización de los sistemas judiciales. De ahí que desde mediados de la década de los noventa, una de las preocupaciones era desarrollar estrategias de fortalecimiento en el sector justicia, a través del uso de las TIC para garantizar el acceso a la justicia desde sitios de difícil acceso, tal y como lo señala un estudio comparado de la justicia en países iberoamericanos (Fabra-i-Abat et al., 2006). Para ese entonces, 18 estados iberoamericanos ya publicaban información sobre la organización del poder judicial, normatividad, diarios oficiales y jurisprudencia a través de las TIC. Diez de aquellos países ofrecían información sobre los procesos judiciales (requisitos, procedimientos, plazos, entre otros) y sobre los servicios prestados (certificados, trámites, entre otros.). También, en la mayoría de los países se facilitaba tanto el intercambio de datos entre operadores jurídicos (jueces, magistrados, funcionarios de juzgados y tribunales), como el uso de sistemas de información como apoyo a la gestión de procesos judiciales.

Así por ejemplo, en Argentina la implantación de las TIC en el ámbito procesal comenzó desde mediados de los años noventa, donde se incorporaron el uso de escáneres para digitalizar documentos, el uso de la firma digital, de notificaciones y pagos electrónicos, videoconferencia, entre otros; sin embargo, solo hasta el año 2011 surgió la Ley de Expediente Electrónico N° 26.685 para darle sustento jurídico al uso judicial de las TIC (Amoni Reverón, 2013).

En Colombia, desde 1995 se ejecutó la estrategia de "Sistematización del ejercicio de la función judicial y la administración de justicia" con el ánimo de adquirir equipos, desarrollar sistemas de información para la gestión de los procesos judiciales, adquirir la infraestructura de red para todos los despachos judiciales y capacitar a los servidores judiciales (Consejo Superior de la Judicatura, 1994). En 2010, a través de la Ley 1394 de 2010, que determina el arancel judicial y nutre de recursos para la descongestión judicial, se ordenó a la Sala Administrativa del Consejo Superior de la Judicatura la articulación de un plan para la inversión de estos recursos, sea esta la ocasión de gestionar un plan meticuloso para la justicia digital, lo anterior como lo señala Londoño-Sepulveda, (2010) por que para ese año se contaba con un sistema de información que permite la visualización de las actuaciones ordenadas por fecha aunque de manera limitada. En 2012, el Código General del Proceso Ley 1564 de 2012 determinó el uso de las TIC en todas las actuaciones judiciales, las cuales se podrán realizar a través de mensajes de datos en la gestión y trámites de los procesos judiciales. En 2014, a través de la Ley 1709, se estableció que en todos los establecimientos penitenciarios, se deben garantizar las locaciones y elementos tecnológicos necesarios para la realización de audiencias virtuales y, de manera preferente los jueces realizarán estas audiencias[5]. El Decreto 806 de 2020 mediante el cual el Gobierno Nacional en el marco de la Emergencia Económica, Social y Ecológica por el COVID 19, adoptó medidas transitorias para el acceso a la justicia a través de medios virtuales y agilidad en los procesos judiciales una de las

[5] Según el Centro de Documentación Judicial - CENDOJ en el año 2010 se realizaron 90 audiencias virtuales, desde entonces se han incrementado en un alto porcentaje, en 2018, se realizaron 10050 y en el primer semestre del año 2019 se realizaron un total de 6.021 (INPEC - Subdirección de Planeación, 2019)

principales medidas que se adoptan son el uso de las TIC en los procesos judiciales (Presidencia de la República de Colombia, 2020). En Colombia la acción constitucional de tutela es el mecanismo más inmediato de protección de los derechos fundamentales constitucionales cuando son vulnerados o amenazados por la acción u omisión de autoridad pública, es así como a diario a los tribunales y juzgados del país llegan miles de tutelas que congestionan el sistema judicial, motivo de preocupación toda vez que por ejemplo, en promedio entre 2015 y 2019 se reciben 726.300 tutelas anualmente (Consejo Superior de la Judicatura, 2019). Es por esto, que la Corte Constitucional anunció la adopción de un programa de inteligencia artificial como iniciativa pionera de un sistema predictivo de detección inteligente de sentencias e información llamado "Pretoria" [6] para facilitar el trabajo de los jueces, el cual es capaz de agrupar, analizar, y clasificar información de las más de 2.700 sentencias diarias que recibe la Corte (Estevez, Fillotrani, & Linares Lejarraga, 2020).

En el año 1993, el Poder Judicial de Costa Rica inicia el proceso de modernización. Del año 2000 se ha venido realizando avances significativos tanto en cobertura nacional de las herramientas tecnológicas, como en el desarrollo de nuevas y mejores formas de gestión judicial, implementando además una gama de servicios electrónicos orientados hacia el usuario (Morales-Navarro, 2011).

En la República Bolivariana de Venezuela, desde 2000, la sala constitucional, mediante sentencia 656 de 2000 estableció la necesidad de adaptar el ordenamiento jurídico a las

[6] Este sistema se basa en "Prometea" que fue desarrollado por el Departamento de Inteligencia Artificial de la Universidad de Buenos Aires (UBA) con el apoyo jurídico de la Facultad de Jurisprudencia de la Universidad del Rosario en Colombia. Sin esta tecnología, una sola persona puede leer sólo 30 expedientes para encontrar patrones similares y clasificarlos según la prioridad de los despachos judiciales.

nuevas realidades sociales, es decir en un entorno virtual, desde la óptica técnica y jurídica, los escritos pueden redactarse, firmarse, remitirse al tribunal y archivarse en formato electrónico, ya que así lo autoriza el Decreto Ley sobre Mensajes de Datos y Firmas Electrónicas de 2001, a pesar de la inexistencia de una regulación especial para tal fin (Amoni Reverón, 2013). Ahora bien, en Venezuela, no hay regulación explícita que permita el uso de videoconferencias en el sistema judicial. Sin embargo, la Ley Orgánica contra la Delincuencia Organizada y el Financiamiento del Terrorismo de 2012 contempla el uso de la videoconferencia cuando no sea posible o conveniente la comparecencia de una persona para un proceso que se esté desarrollando en otro estado; el Código Orgánico Procesal Penal de 2012 permite las notificaciones electrónicas incluyendo aquellas que se realizan por videoconferencias y la Ley Orgánica del Tribunal Supremo de Justicia de 2010, da la posibilidad del empleo de cualquier tipo de TIC en los procesos judiciales que se lleven a cabo ante él (Amoni Reverón, 2013).

En Perú, a través de la Ley 27419, desde el año 2001 proceden las notificaciones judiciales mediante fax, teléfono, o por la vía electrónica; en 2014 se ha establecido en la legislación penal la práctica de audiencias virtuales. Desde 2016, se aplica en todos los distritos judiciales y su uso se ha extendido en asuntos de derecho de familia, para evitar el desplazamiento nacional e internacional de numerosos justiciables en casos vinculados a dicha materia (Quispe Angulo, 2018; Rojas Quispe, 2014).

En Brasil en 2006, a través de la Ley 11.419 se aprobó el uso del expediente electrónico que se aplica en todo tipo de procedimientos judiciales, laborales y administrativos. Sin embargo, otras TIC fueron incluidas desde 1951. Posteriormente, mediante la Ley No. 11.900

de 2009, autorizó el uso excepcional de la videoconferencia, en los procesos penales, para el interrogatorio de los procesados privados de la libertad (Amoni Reverón, 2013; Freire Pimentel, Mateus, & Mendes Saldanha, 2017).

En México en 2009, a través de una serie de reformas a la Ley Federal de Procedimiento Contencioso Administrativo se dio origen al Sistema de Justicia en Línea, el cual a partir de 2011 permite substanciar en todas sus partes un procedimiento jurisdiccional (Chávez, 2011).

El Salvador en el año 2015, la Asamblea Legislativa, aprobó la realización de audiencias virtuales a procesados por el sistema de Justicia, con el fin de no interrumpir procesos penales. Está dirigida muy especialmente para la población privada de la libertad y tiene como objetivo obtener eficacia y rapidez en los procesos penales. Las primeras audiencias se iniciaron en 2016, aunque han presentado varios problemas relacionados con la falta de infraestructura y capacitación de los servidores judiciales (Asamblea Legislativa El Salvador, 2015).

Como se ha podido observar, los tribunales latinoamericanos han invertido tiempo y fondos nacionales en su automatización. Por lo anterior, la incorporación de las TIC, para los países de la región ha constituido una oportunidad para consolidar la eficacia y eficiencia en los procesos judiciales, para estrechar un vínculo permanente del Estado con los ciudadanos, asimismo, para fomentar la participación ciudadana en los procesos judiciales y hacer transparente la información pública como arma contra la corrupción (J. Caballero, de Gracia, & Hammergren, 2011; Ríos Ruiz, 2017). Sin embargo, pese a estos esfuerzos, Beauchard (2016) y Hammergren, (2011) coinciden en que dicha automatización no se ha utilizado para crear bases de datos mejoradas, sino para el procesamiento de textos de documentos

ordinarios (documentos tradicionales escaneados) razón por la cual existe ausencia del flujo de datos sobre los casos, lo cual imposibilita evaluar los impactos.

Por su parte en Europa, se han apoyado iniciativas de justicia digital que van desde la creación de un portal de red judicial en materia civil y mercantil en 2003, hasta la implementación de un atlas de justicia penal y civil, todas ellas tratando de reducir la complejidad de la interacción entre la regulación, la tecnología y las organizaciones (Comisión Europea, 2010; Velicogna, 2017). De las muchas iniciativas que han visto la luz en últimos años en el campo de la justicia digital, en Europa, Estados Unidos y Canadá, una de las más controversiales es el uso de los ODR (Duaso- Calés, 2011; Mania, 2015; Palmgren, 2018).

En Canadá los ODR han implementado el uso de la Inteligencia artificial en los procesos de decisión de los jueces, en especial para ayudar en la negociación y la toma de decisiones, más que en su capacidad de actuar como sustituto de un abogado o un abogado o el juicio de un tomador de decisiones (N. Vermeys & Acevedo-Lanas, 2020). Por su parte, Susskind, (2019) sostiene que estos sistemas de tribunales en línea desplazarán a muchos litigios convencionales, y seguramente la inteligencia artificial, el aprendizaje automático y la realidad virtual probablemente dominarán el servicio judicial. Sin embargo, el uso de los ODR en los países en desarrollo, es marginal, en general, se resuelven mejor los conflictos por presión comunitaria que mediante el acceso a los sistemas de justicia (Beauchard, 2016).

En suma, estos son ejemplos que muestran cómo las TIC han dejado de ser una simple herramienta de soporte para convertirse en una herramienta de resolución de conflictos completamente en línea (García Barrera, 2018).

Ahora bien, en la región Iberoamérica, el debate sobre ciberseguridad derivada del uso de las TIC en la justicia ha estado presente, en las cumbres iberoamericanas de presidentes de cortes supremas y de tribunales superiores de justicia. Especial mención tiene la cumbre realizada en 2018, dónde se creó una red de cooperación en materia de ciberseguridad entre los países miembros de la Cumbre, con el objeto compartir las mejores prácticas para facilitar la socialización de experiencias, evitar el desgaste de esfuerzos y fortalecer las capacidades ante las amenazas cibernéticas (Cumbre Judicial Iberoamericana Edición XIX, 2018).

4.4. TIC, riesgos cibernéticos y las recomendaciones para afrontarlos según etapas de un proceso judicial

A continuación, para las etapas de gestión del proceso judicial, presentación de pruebas o evidencias, decisión judicial y ejecución de sentencias se describirán las TIC en las que se suelen apoyar, los riesgos cibernéticos que ellas conllevan y las recomendaciones para afrontarlos.

4.4.1. Etapa de gestión del proceso.

En la etapa de la gestión del proceso judicial, la RSL encontró que las TIC más mencionadas están los sistemas de información, las videoconferencias y los ODR. Los sistemas de información son el medio de los cuales se automatizan los procesos que contienen tareas reiterativas, permiten capturar, analizar y comunicar la información asociada al expediente judicial para la operación de los procesos (Maestropiedra, 2012; Rosa et al., 2013). También se encuentran las bases de datos jurisprudenciales, accesibles vía portales (Canivet, 2016; Sánchez-Torres, 1998). El almacenamiento, análisis y comunicación de la información dan lugar al uso de otras TIC como las redes, los servidores, el almacenamiento en la nube.

A lo anterior, se suman el uso de portátiles, *tablets*, teléfonos inteligentes, que los servidores judiciales pueden usar para avanzar en sus tareas. El uso de sistemas de información trae múltiples beneficios, entre otros, están el incremento de la efectividad del sistema judicial, la disponibilidad de la información en tiempo real tanto para los usuarios como para los servidores judiciales, reducción de tiempos. Sin embargo, se presenta como riesgo el confiar demasiado en el sistema de información, evitando asumir responsabilidades relacionadas con los deberes de los servidores judiciales. Los sistemas de información son una herramienta para ayudar con el trabajo, para realizar sus tareas, pero no reemplazan la intervención humana (Rosa et al., 2013)

Por su parte, las videoconferencias no son nuevas en el sistema judicial, como lo señala Bellone, (2015), en el sistema judicial estadounidense se ha utilizado desde 1970. La videoconferencia es una tecnología interactiva que transmite datos de audio vídeo y otro tipo para que dos o más partes puedan comunicarse entre sí (Davis et al., 2015; Lillo Lobos, 2011). En otras palabras, lo anterior da lugar a las audiencias virtuales, las cuales pueden definirse como la utilización de los medios técnicos, para la presencia virtual de personas que permita disponer desde otro sitio las personas requeridas para adelantar diligencias en los procesos judiciales (Consejo Superior de la Judicatura, 2014). La mayoría de los países desarrollados incluidos Australia, Canadá, Reino Unido, Singapur, desde ya hace tiempo hacen uso intensivo de las videoconferencias en los procesos judiciales (Devoe & Frattaroli, 2006).

Varios autores como Amoni Reverón, (2013), Bellone, (2015), Davis et al., (2015) concuerdan que es vital que éstas sean de alta calidad técnica en la conexión para que la

comunicación sea fluida, sin interrupciones, en las que se permita que el juez y los demás sujetos procesales se observen y escuchen con detalle, al mismo momento en que se producen sus manifestaciones, como si estuvieran uno frente al otro.

Entre los beneficios que las videoconferencias traen para los procesos judiciales, están: se incrementa la versatilidad y facilidad en la gestión, se amplía el acceso a la justicia por parte de la ciudadanía por la posibilidad de acceder desde diferentes lugares sin desplazamientos, aumenta la seguridad en la medida en que se evitan los desplazamientos de cierto tipo de individuos de la población privada de la libertad; se facilita la mediación de informes de expertos al no incurrir en los costos de tiempo y dinero generado por los desplazamientos; se plantea una innegable posibilidad de incremento en la capacidad de respuesta efectiva a necesidades del sector justicia y su acción interinstitucional (Aaltonen et al., 2015; Aubert, Babin, & Aqallal, 2014; Bellone, 2015; Devoe & Frattaroli, 2006).

Entre las preocupaciones de usar las videoconferencias están (Amoni Reverón, 2013; Bellone, 2015; Davis et al., 2015): i) los problemas técnicos por fallos de la tecnología, los cuales pueden frustrar a jueces, magistrados, abogados y clientes. Los retrasos entre audio y visual son molestos. Las cámaras causan dificultades, pues las personas actúan de manera diferente frente a ellas; ii) las dificultades técnicas pueden afectar la capacidad del acusado de confrontar a testigos en su contra o reprimir la evaluación de un investigador de la confiabilidad de un testigo. Esta evaluación puede hacer que la videoconferencia sea particularmente inadecuada para situaciones en las que un testigo tiene problemas para hablar con claridad o aprendió inglés como segundo idioma; iii) las audiencias de baja calidad por videoconferencia pueden tener un efecto perjudicial en la medida en que pueden conllevar a

percepción de injusticia; iv) la confianza entre el abogado defensor y su cliente puede perderse, subyace la pregunta de si es igual de efectiva como con el proceso cara a cara.

Por otra parte, los ODR son mecanismos alternativos para resolución de conflictos, tales como la mediación, el arbitraje, la facilitación de diálogo, etc., a través de las TIC, en los cuales no intervienen los jueces, donde suelen resolverse conflictos de pequeñas cuantías que evitan sobrecargar el sistema judicial (Mania, 2015; Palmgren, 2018). En consecuencia, los ODR permiten el procesamiento rápido de la información; disminuir los tiempos de desplazamientos disminuyendo las barreras de acceso a la justicia y las diferentes jurisdicciones, con lo que se amplía la cobertura, muy especialmente, si se da la posibilidad de usar una red social como Facebook, como mecanismos alternativo (Al Swelmiyeen & Al-Nuemat, 2017; Mania, 2015).

Los sistemas judiciales estatales son guardianes de los datos confidenciales para individuos y organizaciones. Cuando se trata de activos de datos digitales, los sistemas de los tribunales estatales no son diferentes a las instituciones financieras, las empresas minoristas, los proveedores de atención médica y otras organizaciones gubernamentales. Esta extraordinaria responsabilidad pública los convierte en un objetivo de alto valor para los cibercriminales (Mclaughlin, 2018).

En ese sentido, la RSL permitió identificar varios riesgos cibernéticos asociados a las TIC que se involucran a esta etapa del proceso judicial digital, entre ellos están:

i) Alteración de la información cuando se realizan cambios en el contenido de una base de datos, o se adicionan registros, sin importar que las bases de datos o los sistemas de

información se encuentren On-premises o en cualquiera de las modalidades de almacenamiento en la nube (B. A. Jackson et al., 2016a; Rosa et al.,2013).

ii) Ataques avanzados de amenazas persistentes o *Advanced Persistent Threat* - (APT) y Ataques de inyección de código (ACI): Los APT intentan mantener el acceso continuo y extendido a una red reescribiendo continuamente códigos maliciosos -*malware*- y utilizando técnicas sofisticadas de evasión. Un ataque APT exitoso resulta en un control invisible completo de los sistemas de información durante un período de tiempo prolongado. Por su parte, los ataques de inyección de código implican el envío de código incorrecto a los sistemas de información o a las bases de datos. A través de estos ataques, los ciberdelincuentes engañan al sistema objetivo para que ejecute un comando o permita el acceso a datos no autorizados. El ataque de inyección de código más común utiliza el lenguaje de consulta estándar a bases de datos (SQL), aunque también se encuentra en consultas LDAP, Xpath o NoSQL; comandos del sistema operativo; analizadores sintácticos de XML; cabeceras SMTP; parámetros de funciones; entre otros (Mclaughlin, 2018).

iii) Fallos en la seguridad de la información: Una preocupación natural de las partes es que revelen la información que se usa en un proceso judicial es asegurarse de que sólo se use para un propósito específico y no se divulgue o acceda innecesariamente, preocupación que se agrava cuando se almacena y transmite electrónicamente. Máxime cuando el propósito de un ciberataque es obtener información clasificada y sensible para ganar una ventaja y realizar daños en infraestructura critica (B. Jackson et al., 2016a; Landwehr et al., 2012; Norris Rodin & Rodin, 2015).

iv) Fallos en los intercambios de información: este riesgo está asociado con los problemas

de intercambio de información entre los participantes de los procesos judiciales, incluidos los jueces que obtienen información sobre los procesados o los abogados que obtiene acceso completo a los archivos (B. Jackson et al., 2016b).

v) *Hackeo* de las sesiones de videoconferencias para sabotaje, puede darse por personas externas cuando se quiere hacer daño a la infraestructura crítica relacionada con la justicia o puede darse por parte de los sujetos procesales (Akın Ünver, 2018).

vi) *Phishing:* utiliza la ingeniería social para solicitar información personal de usuarios desprevenidos para comprometer sus propios sistemas. Los correos electrónicos de *phishing* parecen legítimos y manipulan a los usuarios para que ingresen elementos, como nombres de usuario o contraseñas, que pueden usarse para comprometer las cuentas. El *spear-phishing*, un método más personalizado, podría apuntar a jueces y empleados judiciales específicos (Mclaughlin, 2018).

vii) *Ransomware* infecta el software y bloquea el acceso de una organización a sus datos hasta que se paga un rescate. A través de correos electrónicos de *phishing*, descargas automáticas y vulnerabilidades de software sin parches, los ciberdelincuentes intentan extorsionar a los usuarios encriptando sus datos hasta que se cumplan ciertas condiciones. El resultado es una pérdida de datos temporal o incluso permanente. La posibilidad de robo de información asociada al proceso judicial, afecta la credibilidad en el mismo (Mclaughlin, 2018; N. Vermeys & Acevedo-Lanas, 2020).

viii) Robo de información biométrica relacionados con la voz y visualización de rostros durante las audiencias virtuales (Akın Ünver, 2018).

ix) Violación de la privacidad en el contexto de la publicación de los procesos judiciales digitales: La mayor accesibilidad a los informes legales que pueden ofrecer las TIC

significa que cualquier información personal contenida en el informe del proceso puede obtenerse más fácilmente. Además, es importante que exista algún método por el cual se pueda determinar de manera confiable el autor de un documento electrónico. En particular, para que una comunicación se base en ella, debe ser posible demostrar con un alto grado de certeza que un documento no ha sido alterado de alguna manera (Landwehr et al., 2012). Este riesgo también surge cuando se usan los ODR mediante redes sociales como Facebook, la información que allí se comparta se convierte en un tema público (Al Swelmiyeen & Al-Nuemat, 2017).

Entre las recomendaciones para mitigar los posibles ataques, que se pueden extraer de la RSL, están:

Para proteger la información el sistema judicial debe enfrentarse con una mayor coordinación interna y colaboración entre los juzgados y tribunales. A través de este proceso, los tribunales pueden establecer un marco de gobernanza de datos que por una parte, proteja la privacidad de todos los involucrados en el proceso judicial (Hollywood, Boon, Silberglitt, Chow, & Jackson, 2015a; Mclaughlin, 2018) y de otra le dé mecanismos a la Administración de Justicia para sacar provecho de esa información y ser eficiente (Hammergren, 2011). Es conveniente, para apoyar la protección la inclusión de mecanismos como las firmas digitales, el archivo seguro de documentos digitales y el estampado cronológico de mensajes de datos, entre otros (Rincón-Cárdenas, 2013).

Es necesario establecer qué información de los procesos judiciales digitales realmente se debe compartir con el público. Para ello se requiere que la información sea clasificada (N. Vermeys, 2016) y diseñar los sistemas de información con el principio de "minimizar" la

cantidad de información personal que procesa. Desde una perspectiva de ciberseguridad, la estrategia de minimizar puede contribuir a reducir el área de impacto de las violaciones de datos resultantes de ataques cibernéticos o incidentes (Bonfanti, 2018). Es tener en mente el enfoque de protección de datos "por diseño", que se refiere a la adopción de soluciones técnicas, tecnológicas u organizativas relevantes y ad hoc que refuercen la privacidad en las especificaciones de diseño y la arquitectura de sistemas y procesos. Otra opción es el diseño de los sistemas de información con métodos ágiles que rápidamente podrían mostrar las debilidades de un sistema (Tomlinson, 2019).

Un camino, que es subvalorado por los especialistas de ciberseguridad, es promover la cultura de la privacidad y la protección de los datos personales, tanto en las organizaciones como en los individuos. Como lo señala Bonfanti, (2018), el reto es que los sujetos procesales junto con los jueces y los abogados tengan la capacidad de proteger directa o indirectamente el ciberespacio, donde se mueve la información jurídica. Algo no menor, desde la perspectiva, implica que hay respeto por ello y que se requiere regulación.

Aunado a lo anterior, se requiere trabajar en disminuir la carencia de habilidades informáticas genéricas y específicas de los usuarios internos del sistema judicial como de los ciudadanos en general (Rosa et al., 2013). Máxime si se considera que según Devoe & Frattaroli, (2006) los abogados y servidores judiciales les toma tiempo adoptar la tecnología por ser muy conservadores, por ello, es necesario la capacitación de manera continua.

Para disminuir los riesgos por el uso de la videoconferencia en los tribunales, Bellone, (2015) aclara que es importante que se actualicen continuamente los equipos de

videoconferencia, se establezcan procedimientos de estandarización para el uso de videoconferencia y limitar el uso de las videoconferencias a diligencias judiciales. El mismo autor sugiere que se capacite continuamente a los servidores judiciales, no sólo en los aspectos técnicos del uso de los equipos de videoconferencia sino en las estrategias para generar confianza y entendimiento entre los sujetos procesales.

Es necesario ser conscientes que existen elementos facilitadores e inhibidores para compartir información entre agencias estatales. Entre los facilitadores están la capacidad de infraestructura tecnológica, la seguridad y privacidad de la información, las lecciones aprendidas de otros proyectos, la confianza, el conocimiento de la entidad, la voluntad política de las entidades, y los beneficios percibidos. También es importante diagnosticar las capacidades de intercambio de información en el sector justicia para apoyar la toma de decisiones eficaz y eficiente, incluido el análisis de delitos en tiempo real (Clark, 2017). Por su parte, en los inhibidores se encuentran la capacidad del personal de TI, la confianza entre las entidades, el financiamiento, y el cumplimiento de la normatividad (Hogeveen, 2020; Rico- Pinto & Sánchez-Torres, 2019; Treglia & Park, 2009). También Banks, Hollywood, Woods, Woodson, & Johnson, (2016) recomiendan compartir más información entre los tribunales para que los datos no puedan "pasar por alto" entre las jurisdicciones y para desarrollar formatos de consenso para los datos digitales utilizados en los tribunales y, así evitar problemas de incompatibilidad.

Para garantizar que la información sea confiable es importante el uso de estándares y la capacitación para garantizar que los datos se capturen de manera adecuada y precisa (Rosa et al., 2013).

Para garantizar el acceso controlado a los sistemas de información (Stockman, 2014) recuerda aspectos como: la responsabilidad por parte del personal de Tecnologías de la Información de la protección de sus cuentas como administradores; dado que la mayoría de los delincuentes usan las cuentas de otros para sus ataques, las organizaciones podrían implementar la autenticación multifactor en sus entornos. Esto implica usar más que un nombre de usuario y contraseña para acceder; los escaneos biológicos y las contraseñas únicas enviadas como mensajes de texto a teléfonos celulares son algunos ejemplos; y, por último, no olvidar incrementar la detección de riesgos a través del monitoreo de los logs de actividades.

4.4.2. Etapa de presentación de pruebas o evidencias

Cuando la evidencia electrónica empezó a ingresar, el sistema judicial se enfrentó a la tarea de evaluar la admisibilidad de dicha evidencia, la cual hoy afortunadamente es aceptada (Bachman, 2014; Zimmerman, 2013). La evidencia digital para el estudio de los casos, sin importar la jurisdicción, tiene múltiples orígenes.

Por ello, la RSL permitió identificar que las fuentes más comunes de evidencia son los correos electrónicos, audios y videos (Hollywood, Boon, Silberglitt, Chow, & Jackson, 2015b; Hollywood, Woods, Lauland, Jackson, & Silberglitt, 2018). Por otra parte, también se identificó que otras fuentes menos comunes son el uso de simuladores computacionales, y el uso de realidad virtual, que llevan tiempo siendo contemplados (Clifford & Kinloch, 2008). En Estados Unidos es usual que a través del modelado holográfico virtual en 3D o animaciones forenses, se recreen las escenas del crimen, a partir de la opinión de los sujetos

procesales, lo cual permite que aclarar a todas las partes los hechos, promueve la solución pronta gracias a la ilustración de los casos y convencer con argumentos a quienes toman la decisión (Clifford & Kinloch, 2008; Horan & Maine, 2014).

La RSL también señaló que se encuentra la evidencia recolectada a través de drones, cámaras de video, imágenes satelitales, cámaras térmicas, dispositivos con geoposicionamiento espacial, y los nuevos dispositivos que se desarrollen gracias a la incorporación de sensores portátiles o no conectados a Internet, conocido como el internet de las cosas -IoT por sus siglas en inglés (Akın Ünver, 2018; Hollywood, Woods, Silberglitt, Book, & Jackson, 2015; Lanier & Cooper, 2016).

Por último, se encontró que con el advenimiento del análisis de la analítica de datos, las agencias de inteligencia y de aplicación de la ley examinan rutinariamente cantidades masivas de lo que muchos consideran datos privados o personales, a través de las búsquedas en las redes sociales, los cuáles también han empezado a ser consideradas como una posible fuente de evidencias (Kalemi & Yildirim-yayilgan, 2016; Lanier & Cooper, 2016).

En general el beneficio de estas TIC señaladas es que reducen los tiempos, los costos del proceso de aportar las evidencias (Clifford & Kinloch, 2008; Lanier & Cooper, 2016). Aunque una preocupación natural es la falta o poca confianza en la tecnología y, por ello, se corre el riesgo que algunas pruebas puedan ser inadmisibles dentro de los procesos judiciales (Clifford & Kinloch, 2008; Ewald, 2019; Zimmerman, 2013).

De acuerdo con la RSL revisión se encontró que, el uso de las anteriores TIC, pueden ocasionar los siguientes riesgos cibernéticos:

i) Alteración de la información: Dado que el principal papel de estas tecnologías es recolectar evidencia, cualquier adulteración incidiría en la decisión que posteriormente, el juez tome, por ello, es importante su protección (Coudert, Butin, & Le Métayer, 2015; Lanier & Cooper, 2016).

ii) *Hackeo* de los dispositivos: Dada la recolección de los patrones de comportamiento de individuos y organizaciones con las TIC los hackers pueden usarlas para espiar o dañar a individuos u organizaciones (Akın Ünver, 2018).

iii) Robo de la información y daños a la reputación: Las TIC antes mencionadas permiten recolectar información biométrica sensible, es decir, las huellas dactilares, las características de la voz, los rostros, la retina y los termogramas, por ello es importante evitar que caigan en manos criminales (Akın Ünver, 2018). Además, se encuentra el robo de información propiedad de las organizaciones, si ella es robada, puede afectar la reputación y en consecuencia afectar negativamente los precios de las acciones o reducir el consumo confianza en una organización (Cukier, Maimon, & Berthier, 2012).

iv) Violación a la privacidad: Tecnologías como drones, cámaras de video, imágenes satelitales, cámaras térmicas, dispositivos con geoposicionamiento espacial, y los dispositivos basados en IoT recolectan bastante información sobre los patrones de comportamiento de individuos y organizaciones, por ello se presentan el dilema relacionado con el deber de informar a las personas filmadas, el tiempo y el contenido de las grabaciones (Lanier & Cooper, 2016). Este riesgo también es propio de la evidencia recolectada desde las redes sociales, resaltan la necesidad de una mayor educación, leyes y políticas para garantizar que estos sitios y la difusión de información

estén bajo la autoridad de la policía al tiempo que protegen los derechos del público (Kalemi & Yildirim-yayilgan, 2016; Lanier & Cooper, 2016).

Las recomendaciones que la RSL evidenció son: i) es imperante el cuidado y la protección de las evidencias de los procesos, no sólo las que per sé son digitales, sino del proceso de conversión de las evidencias análogas a digitales para evitar las brechas "decisionales" que pueden existir entre quien colecta la evidencia y quien la usa para la toma de decisiones (Ewald, 2019; Hollywood, Woods, et al., 2015); y, ii) el sistema judicial debe tratar grandes cantidades de datos, volumen que crece día a día, por lo que, debe tener las capacidades de talento humano y recursos financieros y de infraestructura necesarios para manejar ese volumen de datos (Goodison, Davis, & Jackson, 2015; B. A. Jackson et al., 2016b).

4.4.3. Etapa de decisión judicial

En la etapa de la decisión judicial, la RSL encontró que las TIC que se usan, además de las ya señaladas en las otras etapas, están los sistemas basados en técnicas computacionales de minería de textos, de analítica de datos (conocida como *legal analytics*), y de inteligencia artificial como el aprendizaje de máquina supervisado o el uso de *chatbots*.

La minería de textos junto con el aprendizaje de máquina supervisado ha permitido el desarrollo de sistemas predictivos que usan los textos de decisiones judiciales de casos ya juzgados, que pueden ofrecer a los abogados y jueces una herramienta útil de asistencia, en la preparación de los casos para los primeros, y en la toma de la decisión judicial para los segundos (Aletras, Tsarapatsanis, Preoţiuc-Pietro, & Lampos, 2016).

Por su parte, la analítica de datos aplicada al ámbito jurídico, es decir, el procesamiento

de altos volúmenes de información, combinada con el aprendizaje de máquina supervisado han sido utilizados para desarrollar sistemas que permiten analizar miles de sentencias para: i) identificar patrones y elementos claves en casos judiciales similares al que se esté analizando como insumo para las decisiones como es el caso de la Fiscalía en Argentina, de la Corte Constitucional en Colombia o del sistema judicial en China (Estevez et al., 2020; Li, Sheng, Ge, & Luo, 2019; Prins, 2018); ii) predecir las posibles formas de decisión de un tribunal o juzgado con base en las decisiones previas en Francia, Canadá, o Corte Interamericana de Derechos Humanos (Martin Katz, Bommarito, & Blackman, 2017; Şulea, Zampieri, Vela, & Van Genabith, 2017; Westermann, Walker, Ashley, & Benyekhlef, 2019); iii) ayudar en la negociación y en el arbitramiento ofreciendo diferentes posibilidades a través de los ODR como en Canadá (Benyekhlef, 2018; N. Vermeys & Acevedo-Lanas, 2020); iv) para fijar las fianzas y sentencias basadas en el riesgo, a partir de los datos disponibles de los sujetos procesales (Hollywood et al., 2018). La analítica de datos, también se combina con el uso de Chatbots basados en técnicas de Inteligencia Artificial, como el procesamiento de lenguaje natural, y *deep learning*, que conversan en términos humanos, los cuales interactúa con abogados y jueces para orientar y brindar ideas potenciales para establecer un paralelismo entre casos y, al mismo tiempo, responder y obtener y derivar conocimientos relevantes de la enorme cantidad de datos legales (NU., GK., GS., RamasubramanianK., 2020).

Varios de estos sistemas han incursionado usando computadoras cuánticas para disminuir los procesos de procesamiento y apoyar los procesos de decisión (Castell, 2018).

Los beneficios de usar estas técnicas computacionales es que se reducen sustancialmente los tiempos de análisis de datos, por parte, tanto de los sistemas de información usuales, como

de los servidores judiciales involucrados (Estevez et al., 2020; N. Vermeys & Acevedo-Lanas, 2020). Sin embargo, existen preocupaciones propias del uso de la Inteligencia Artificial en la medida que existe la posibilidad de que se den sesgos, cuando los sistemas están aprendiendo, en detrimento de ciertas poblaciones (N. Vermeys & Acevedo-Lanas, 2020). Hay otras preocupaciones, también, propias del uso de la Inteligencia Artificial relacionadas con la propiedad intelectual digital, el cumplimiento de los derechos humanos y la ética (Li et al., 2019). Algunos consideran que el uso de las TIC en la etapa de decisión judicial tiene como riesgo que los juzgadores podrían quedar definitivamente aislados y privados de toda capacidad de influencia en el proceso judicial (García Barrera, 2018).

La RSL permitió identificar varios riesgos cibernéticos asociados a las TIC que se involucran en la etapa de decisión judicial, entre ellos están (Li et al., 2019): i) alteración de la información, ii) robo de la información del proceso, iii) robo de información sensible, y, iv) violación de la privacidad, medida que se revele información de las decisiones judiciales antes de ser proferidas.

Entre las recomendaciones para mitigar los posibles ataques, que se pueden extraer de la RSL, están: i) que los sistemas tengan acceso únicamente a los datos a los que es estrictamente necesario, que no los almacene, ni modifique, ni realice copia de los mismos (Estevez et al., 2020); que los sistemas aprendan con un conjunto de datos estable que no se actualice constantemente (Li et al., 2019).

4.4.4. Etapa de ejecución de sentencias

En la etapa de la ejecución de las sentencias, la RSL encontró que las TIC que se usan,

además de las ya señaladas en las otras etapas, son los dispositivos que cuentan con sensores como artefactos de lo que se denomina el Internet de las cosas -IoT y los sistemas de información.

Así, están los sistemas de información que están relacionados con la gestión de los establecimientos penitenciarios; los sistemas de seguimiento a través de las pulseras y los brazaletes electrónicos, que son usados en los desplazamientos de la población privada de la libertad, o cuando se les ordena prisión domiciliaria. Estos dispositivos están en pleno auge en distintos lugares del mundo, interactúan, constantemente, enviando y recibiendo datos de geolocalización (Akın Ünver, 2018). Otros sistemas de seguimiento están conformados por los sensores, tanto portátiles como contenidos en la infraestructura, conectados a Internet, la web semántica y a los agentes inteligentes para compartir y analizar las fuentes de datos para apoyar la ubicación y el seguimiento de los delincuentes (Hollywood, Woods, et al., 2015).

También están los sensores biomédicos, los cuales evalúan y monitorean la salud y seguridad de los oficiales que cuidan los centros penitenciarios. Estos sensores deben controlar los niveles de estrés, fatiga y lesiones. Los datos se usan para acortar dinámicamente los turnos de trabajo si los niveles de fatiga son excesivos (Hollywood, Woods, et al., 2015).

Si bien, el principal beneficio del uso de los dispositivos de IoT es que hay control sobre la población privada de la libertad y facilita la gestión de los centros penitenciarios, se manifiesta la preocupación por cierta intromisión del Estado en la intimidad (Akın Ünver, 2018; Banks et al., 2016; Hollywood, Woods, et al., 2015; Lanier & Cooper, 2016).

La RSL permitió identificar varios riesgos cibernéticos asociados a las TIC que se involucran en la etapa de ejecución de las sentencias:

i) Alteración de la información: especialmente de los sistemas de geolocalización para los privados de la libertad buscando engañar al sistema judicial (Akın Ünver, 2018), y de los sistemas de información para la gestión de los establecimientos penitenciarios.

ii) Excesivos esquemas de encriptación: las compañías que producen estos dispositivos IoT, en aras de dar confianza a sus usuarios, los protegen mucho mediante esquemas de encriptación. Sin embargo, en China, Estados Unidos y Rusia se obliga a las compañías a que tengan un mecanismo para que la justicia pueda entrar a desencriptar la información aquí recolectada (Akın Ünver, 2018).

iii) *Hackeo* de los dispositivos IoT. Si bien, el uso de tecnologías como la geolocalización para la población privada de la libertad, facilita el seguimiento y la recolección de bastante información sobre los patrones de comportamiento de individuos y organizaciones los hackers pueden usarlas para espiar o dañar a individuos u organizaciones o incluso hacer daño corporal a quien los use (Akın Ünver, 2018).

iv) Robo de información asociada a la población privada de la libertad o de información biométrica perteneciente a los oficiales de los establecimientos penitenciarios (Akın Ünver, 2018).

v) Violación de la privacidad derivado del uso de las pulseras y brazaletes que constantemente recopilan y envían datos a la red, y ponen en jaque la intimidad de sus dueños (Lanier & Cooper, 2016; Rincón-Cárdenas, 2019).

Entre las recomendaciones para mitigar los posibles ataques, que se pueden extraer de la

RSL, está la necesidad de capacitación para los servidores judiciales de la justicia penal sobre las implicaciones de la seguridad cibernética (Da Luz Batalha, 2013; Hollywood et al., 2018).

4.4.5. Síntesis

Los riesgos más frecuentes que se encontraron en las diferentes etapas del proceso judicial digital son: i) Alteración de la información; ii) Fallos en el intercambio de información; iii) Falta de seguridad de la información transmitida en los procesos judiciales; vi) *Ransomware*; v) Robo de la información del proceso; vi) Robo de la información sensible; vii) Violación a la privacidad. En la Tabla 2 se evidencia por cada etapa del proceso cuáles son los riesgos que se repiten más en cada una.

Tabla 2 Riesgos cibernéticos de las diferentes etapas de los procesos judiciales.

Riesgos	Gestión del proceso	Evidencia o pruebas	Decisión	Ejecución
Alteración de la información		x	x	x
Ataques avanzados de amenazas persistentes (APT)	x			
Ataques de inyección de código	x			
Ausencia de gobernanza de datos	x			
Costo por la recuperación de la información robada	x			
Daños a la reputación		x		
Exceso de esquemas de encriptación		x		
Fallos en el intercambio de información	x	x		
Falta de seguridad de la información transmitida en los procesos judiciales	x	x		
Hackeo de los dispositivos IoT		x		x

Riesgos	Gestión del proceso	Evidencia o pruebas	Decisión	Ejecución
Hackeo de las sesiones	x			
Phishing	x			
Ramsonware	x	x		
Revelación de información secreta o confidencial		x		
Robo de información biométrica	x			
Robo de la información del proceso	x	x	x	x
Robo de la información sensible	x	x		
Spear-phishing	x			
Violación a la privacidad	x	x	x	x

Fuente: Elaboración propia con base en la RSL.

Por su parte, las recomendaciones extraídas de la RSL se pueden agrupar así:

Fortalecer el marco legal. Coincidimos con (Mcmillion, (2013), Pijnenburg-Muller, (2015), Toapanta, Gurumendi, & Gallegos, (2019) en que un marco legal adecuado, es el esqueleto de la ciberseguridad, el cual permita el desarrollo de la ciberseguridad a largo plazo, como dar herramientas que permitan judicializar y castigar a aquellos que atacan a través del ciberespacio. De acuerdo con Kramer & Butler, (2019) a menudo se carece en los países en desarrollo del marco legal adecuado, prueba de ello en un país como Colombia como lo señala Sánchez-Acevedo, (2017) requiere el desarrollo de régimen jurídico para: i) identificación electrónica de ciudadanos, servidores públicos y sedes electrónicas; ii) esquema de interoperabilidad de los sistemas; y, iii) para las tecnologías como la analítica y el big data.

Desarrollar programas de concientización y capacitación. Estos programas se pueden clasificar según a quienes estén dirigidos. Hay un conjunto de programas de concientización y sensibilización dirigido a los servidores judiciales, incluidos jueces y magistrados, y a los abogados en los que se traten las siguientes temáticas (Da Luz Batalha, 2013; Devoe & Frattaroli, 2006; Duaso-Calés, 2011; Rosa et al., 2013; Toapanta et al., 2019): a. las habilidades necesarias para la interacción con las TIC, toda vez que los abogados y servidores judiciales les toma tiempo adoptar la tecnología por ser muy conservadores; b. los riesgos que se dan en el ciberespacio; c. la cultura de la protección de la información y de la privacidad, puesto que es importante que los sujetos procesales conozcan cómo se manejan los datos obtenidos en los procesos judiciales en concordancia con la normatividad existente para evaluar su confiabilidad y manejo y cómo este se articula a la efectiva operatividad judicial.

Otro conjunto de programas de capacitación especializada dirigido al personal técnico de TI, para la gestión de la información, la gestión de riesgos de ciberseguridad a través de la implementación de marcos de ciberseguridad lo que contribuye a incrementar la capacidad del talento humano de equipos de TI (Kramer & Butler, 2019; Mcmillion, 2013; Pijnenburg-Muller, 2015; Rosa et al., 2013). Aunado a lo anterior, se sugiere reclutamiento de personal ya formado para evitar los costos de aprendizaje (Kramer & Butler, 2019).

Incrementar la infraestructura para manejar los ciberataques: Como se mencionó antes, la literatura recomienda, muy especialmente, el desarrollo de buenas prácticas para definir políticas y protocolos en gestión de los riesgos cibernéticos, relacionadas con el marco de ciberseguridad de la NIST en sus funciones de: Identificar a través de la evaluación e

identificación de riesgos; Proteger asociados con la definición de controles de acceso junto con auditorías de usuarios, el otorgamiento o revocación de autorizaciones; y, detectar a través del registro e identificación de incidentes, y análisis de vulnerabilidades.

Para lograrlo y partiendo de que ha habido un aumento de graves ataques informáticos e incidentes de violación de datos, se requiere de destinar partidas presupuestales amplias, que han de ser distintas a los recursos que se destinen a la gestión propia de TIC, que deben cubrir a cada institución del sistema judicial (Chatfield & Reddick, 2017; Grupo e-justicia - Cumbre Judicial Iberoamericana, 2018; Kramer & Butler, 2019). Coincidimos con Kramer & Butler, (2019) y Pijnenburg-Muller, (2015) en cuanto a que la escasez de infraestructura para manejar los ciberataques, combinada con un mayor uso de la tecnología es un asunto apremiante y para evitar que los cibercriminales se aprovechen de la protección inadecuada, o de la falta de preparación de gobiernos e instituciones, es importante el diseño de procesos de simulación de ataques, que pueden estar a cargo de hackers-buenos que están dispuestos a verificar las vulnerabilidades de un sistema o de una organización a través de procesos de simulación de juegos de ataques.

Aunado al fomento de la concientización de sobre la cultura de la privacidad, ya mencionado, es importante que los sujetos procesales conozcan cómo se manejan los datos obtenidos en los procesos judiciales en concordancia con la normatividad existente para evaluar su confiabilidad y manejo y cómo este se articula a la efectiva operatividad judicial, para esto es necesario la coordinación entre abogados, jueces y magistrados y personal de TI, a través del manejo adecuado de la información. Para ello, es necesario saber qué información se puede compartir, qué información es confidencial o reservada, con protocolos muy claros

para compartir información dentro y fuera de las instituciones involucradas (Chatfield & Reddick, 2017).

Aprender de las experiencias de otros: Los desafíos de ciberseguridad continúan evolucionando en alcance y sofisticación, por ende, la necesidad de fortalecer la seguridad de la información de las organizaciones públicas o privadas es común, por lo que se hace necesario comprender los esfuerzos de ciberseguridad, los aprendizajes, y las mejores prácticas por ejemplo en la notificación de incidentes, en las herramientas, en el intercambio de información, entre otros, mediante la innovación abierta. Es decir, a través de alianzas con el sector privado, o con las redes de cooperación con otras entidades públicas nacionales e internacionales (Grupo e-justicia - Cumbre Judicial Iberoaméricana, 2018; Kramer & Butler, 2019; Pijnenburg-Muller, 2015). La innovación abierta, en este caso, además permite una serie de aprendizajes que evitan perder tiempo, recursos, en soluciones que pueden no ser aptas.

Incluso es válido aprender de los ciberatacantes, en la medida en que los cibercriminales son adaptativos, y en consecuencia el terreno cambia constantemente en el dominio cibernético, por lo que debe haber mecanismos para reconocer y ajustarse a las realidades nuevas y prevalecientes, y para incorporarlas y responder rápidamente (Center for Cyber and Homeland Security., 2016).

Sin embargo, toda innovación incremental o disruptiva requiere que se reconozca el impacto de ella dentro de la cultura de las organizaciones y del talento humano que la gestiona. Se debe tener en cuenta la particularidad de cada organización, no es recomendable

tomar las prácticas y replicarlas sin más. Muy especialmente, es fundamental comprender si se facilitan o afectan los valores subyacentes al sistema de justicia (Bailey, 2016; N. W. Vermeys & Benyekhlef, 2011).

4.5.Funciones y subcategorías del marco de ciberseguridad NIST

A continuación, se presenta el análisis de las funciones y subcategorías de la NIST de manera global y clasificadas por las etapas de los procesos judiciales.

4.5.1. Mapeo de las funciones y subcategorías de la NIST

El mapeo de las funciones y subcategorías del marco de ciberseguridad de la NIST reveló el siguiente panorama. En primer lugar, sólo 61 de los documentos seleccionados para esta revisión de literatura, mencionan a las funciones o sus subcategorías de manera directa o indirecta. De hecho, sólo tres documentos, los mencionan directamente, mientras que 58 documentos lo hacen de manera indirecta. Dentro de este universo de documentos, las funciones de Proteger y de Identificar, se destacan al ser mencionadas en un 86,89% y 63,93% de los documentos. Le siguen las funciones de detectar con un 21,3%, recuperar con un 18,03%, y responder con un 13,11% conforme se observa en la Tabla 3.

En la función de Identificar las subcategorías más frecuentes son la Evaluación de riesgos (ID.RA) y el Entorno empresarial (ID.BE); en la función de Proteger las subcategorías más frecuentes son Seguridad de los datos (PR.DS) y Procesos y procedimientos de protección de la información (PR.IP); en la función de Detectar la subcategoría más frecuente es Anomalías y Eventos (DE.AE); en la función de responder, aunque son muy poco mencionadas, se destacan la Planificación de la Respuesta (RS.RP) y la Mitigación (RS.MI);

por último, en la función de recuperación la única subcategoría mencionada, aunque de manera marginal es la Planificación de la recuperación (RC.RP).

En la función Identificar las subcategorías con menor relevancia son las de Estrategia de gestión del riesgo (ID.RM) y Gestión del riesgo de la cadena de suministro (ID.SC); en la función Proteger, son Mantenimiento (PR.MA) y Tecnología de protección (PR.PT); en la función Detectar la subcategoría menos mencionada es Procesos de Detección (DE.DP) ; en la función de Responder no existe mención alguna para las subcategorías de Análisis (RS.AN) y Mejoras (RS.IM); en la función de Recuperar no existe mención para las subcategorías de Mejoras (RC.IM) y Comunicaciones (RC.CO).

Tabla 3. Mapeo de las funciones y subcategorías del marco de ciberseguridad NIST

Función y subcategorías	Número de documentos	Porcentaje
1. IDENTIFICAR (ID)	**39**	**63,93**
1. Gestión de activos (ID.AM)	13	21,31
2. Entorno empresarial (ID.BE)	15	24,59
3. Gobernanza (ID.GV)	11	18,03
4. Evaluación de riesgos (ID.RA)	16	26,23
5. Estrategia de gestión de riesgos (ID.RM)	3	4,92
6. Gestión del riesgo de la cadena de suministro (ID.SC)	-	-
2. PROTEGER (PR)	**53**	**86,89**
1. Gestión de identidad, autenticación y control de acceso (PR.AC)	24	39,34
2. Concienciación y capacitación (PR.AT)	15	24,59
3. Seguridad de los datos (PR.DS)	39	63,93
4. Procesos y procedimientos de protección de la información (PR.IP)	31	50,82
5. Mantenimiento (PR.MA)	3	4,92
6. Tecnología de protección (PR.PT)	2	3,28
3. DETECTAR (DE)	**13**	**21,31**
1. Anomalías y Eventos (DE.AE)	7	11,48
2. Monitoreo continuo de la seguridad (DE.CM)	4	6,56
3. Procesos de Detección (DE.DP)	3	4,92

Función y subcategorías	Número de documentos	Porcentaje
4. RESPONDER (RS)	**8**	**13,11**
1. Planificación de la Respuesta (RS.RP)	4	6,56
2. Comunicaciones (RS.CO)	1	1,64
3. Análisis (RS.AN)		-
4. Mitigación (RS.MI)	4	6,56
5. Mejoras (RS.IM)		-
5. RECUPERAR (RC)	**11**	**18,03**
1. Planificación de la recuperación (RC.RP)	11	18,03
2. Mejoras (RC.IM)		-
3. Comunicaciones (RC.CO)		-

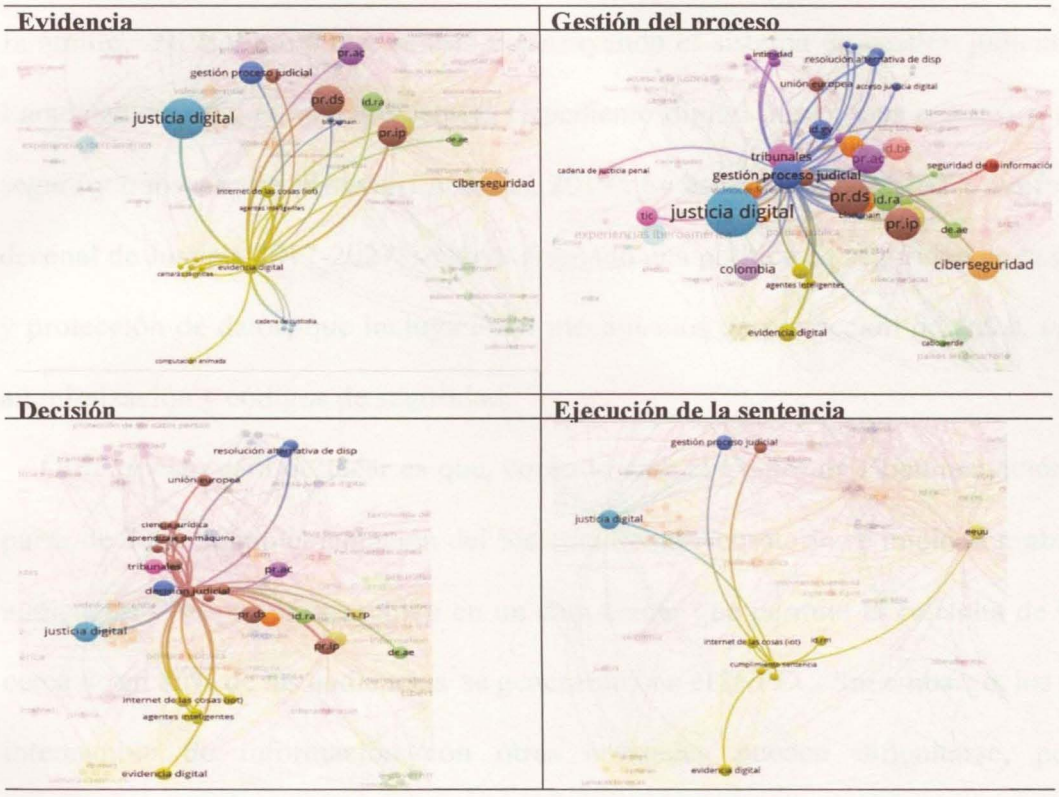
Fuente: elaboración propia.

4.5.2. Mapeo de las funciones y subcategorías del marco de ciberseguridad NIST a la luz de las etapas de un proceso judicial

En relación con el mapeo de las funciones y subcategorías de la NIST con respecto a las etapas de un proceso judicial, se encontró, como se puede observar en la Figura 3 que las subcategorías Seguridad de los datos (PR.DS), Procesos y procedimientos de protección de la información (PR.IP), y Evaluación de riesgos (ID.RA) son las tres más frecuentemente mencionadas en los documentos relacionados con las etapas de evidencia digital, gestión del proceso judicial y de decisión judicial. Le siguen las subcategorías de Gestión de identidad, autenticación y control de acceso (PR.AC).

En la Figura 3 también se observa que en la etapa de gestión del proceso judicial, además de destacan las subcategorías de Entorno empresarial (ID.BE) y Gobernanza (ID.GV). En la etapa de decisión judicial se destacan, también las subcategorías de Planificación de la Respuesta (RS.RP) y Anomalías y Eventos (DE.AE). Por último, en la etapa de cumplimiento de la sentencia, sólo se menciona la subcategoría de Estrategia de gestión de riesgos (ID.RM).

Figura 3. Mapeo de las funciones y subcategorías del marco de ciberseguridad NIST según de las etapas de un proceso judicial.



Fuente: Elaboración propia. Usando el método de co-ocurrencias en VoSViewer

5. Recomendaciones de ciberseguridad para la justicia digital colombiana

Como se señaló en la sección 4.3 el Estado Colombiano ha realizado varios esfuerzos con miras a alcanzar la Justicia Digital. En ese sentido se pueden señalar que para la gestión de los procesos, la Rama Judicial ha desarrollado software internamente como justicia web que es la segunda generación del sistema de información justicia XXI cliente-servidor, los cuales apoyan las estadísticas que sirven de bse para la toma de decisiones, de manera básica pero exitosa (López-Jaramillo, 2019). Sin embargo, aún no se puede hablar de un "modelo de

justicia en línea", como quiera que los sistemas de información son sólo de consulta muy global, es decir, solo se pueden ver el estado del proceso y las actuaciones judiciales (López-Jaramillo, 2019), pese a que se está construyendo el sistema de gestión judicial unificado. Lamentablemente, tampoco existe el Expediente digital único, con registro y trazabilidad segura y transparente (Rincón-Cárdenas, 2019). Se espera que para 2027, conforme al Plan decenal de Justicia 2017-2027, se haya diseñado una política de seguridad de la información y protección de datos, que incluya crear mecanismos de protección de datos, encriptación, anonimización y códigos de seguridad.

Otro aspecto para destacar es que, como lo dice el Centro de Documentación Judicial, a partir de 2006 la implementación del Sistema Penal Acusatorio se inició la grabación de las audiencias y su posterior archivo en un data center que permite la consulta de las mismas, cerca de un 80% de las audiencias se generaron con el INPEC. Sin embargo, los procesos de intercambio de información con otras entidades pueden dificultarse, por la poca implementación de los procesos de interoperabilidad entre las diferentes entidades del sector justicia (Gil Botero, 2019; Rincón-Cárdenas, 2019).

Si bien desde 2012, se admite la evidencia digital, con la expedición del Decreto 806 de 2020 se aceleró la recepción de las pruebas digitales de manera virtual. También se destaca la muy reciente adopción de Pretoria, sistema predictivo de detección inteligente de sentencias e información, para apoyar la etapa de decisión judicial en la Corte Constitucional. Sin embargo, este es el único esfuerzo, en consecuencia el 99% de los despachos judiciales no usa herramientas de analítica de datos, ni tampoco minería de textos, el uso de las TIC es poco. En la etapa de ejecución de sentencias, en la justicia penal, se usan los dispositivos electrónicos con GPS para las detenciones domiciliarias. Sin embargo, no existen sistemas

de información para registrar la cartilla biográfica de la población carcelaria, en consecuencia, los jueces que vigilan las penas no tienen acceso a ella de manera digital.

Por último, es de destacar los avances en el marco legal y que cerca del 28, 6% del total del presupuesto anual del sector justicia en los últimos tres años, se dedica a la inversión en TIC, lo cual demuestra que es un asunto prioritario (Gil Botero, 2019).

Frente a este panorama y como se observó en el análisis de cada etapa del proceso judicial, la RSL permitió evidenciar una serie de recomendaciones en torno a la ciberseguridad en la justicia digital, que sirven de base para las recomendaciones al caso colombiano, las cuales se presentan a continuación:

Si bien es cierto que en Colombia se ha avanzado en el **marco legal** para la ciberseguridad a través de diferentes políticas y mecanismos que se han venido trabajando desde el año 2011, como el CONPES 3701 sobre Lineamientos de Política para Ciberseguridad y Ciberdefensa, la Ley Estatutaria 1581 del 2012, el CONPES 3854 sobre Política Nacional de Seguridad Digital de 2016, el decreto 1008 de 2018, en la medida en que estas políticas y mecanismos se enfocaron en el fortalecimiento y generación de capacidades en el Gobierno nacional, para brindar confianza digital, seguridad y defensa a los ciudadanos, cabe anotar que no se ha logrado el avance esperado en cuestiones de confianza digital y en fortalecimiento del marco legal. Retrasos que dieron a lugar al reciente CONPES 3995 de 2020, sobre Política Nacional de Confianza y seguridad Nacional, del que celebramos su expedición puesto que busca subsanar las falencias mencionadas al establecer medidas para ampliar la confianza digital, mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital.

Para la justicia colombiana garantizar la confianza y seguridad digitales, se constituye en un reto mayor, que de no superarlo iría en un mayor detrimento de la credibilidad del poder judicial. La administración de justicia tiene, entonces, una responsabilidad de generar las medidas necesarias para dar celeridad y confianza a las actuaciones judiciales digitales. Por ejemplo, en la Rama Judicial, el personal de TI se encuentra en la Unidad de Informática, ubicada bajo la Dirección Ejecutiva de la Administración Judicial, del Consejo Superior de la Judicatura -CSJ. Allí se dispone del equipo de TI que atiende las altas cortes, los tribunales y los conglomerados de juzgados. Esa estructura se replica en las diferentes seccionales del CSJ en todo el país. Ello significa que el Director de la Unidad de Informática no tiene la posibilidad de asesorar directamente a quienes toman decisiones para sacar el mejor provecho de las TIC, por ello, pese a que el personal de TI esté capacitado y aplique un modelo de gobernanza de seguridad, se dificulta garantizar que la seguridad de la información sea vista como algo estratégico y relevante. Por ello, sería importante que los lineamientos del Decreto 415 de 2016, que aplican a la Rama Ejecutiva se extiendan a la Rama Judicial de tal forma que, el director de TI, quien tiene la responsabilidad, al más alto nivel de las instituciones, de seguridad de la información, de tal forma que podría establecer una comunicación constante con la alta dirección de la institución, y guiarla sobre la estrategia de seguridad y protección de datos. Adicionalmente, es necesario la propuesta de implementar una política pública que busque un incremento en las capacidades y en las posibilidades de responder de forma adecuada y rápida a los nuevos retos tecnológicos basados en la gobernanza digital para el fortalecimiento de la justicia en el país. Igualmente se requiere el desarrollo de régimen jurídico para: i) identificación electrónica de ciudadanos, servidores públicos y sedes

electrónicas; ii) esquema de interoperabilidad de los sistemas; y, iii) para las tecnologías computacionales basadas en Inteligencia Artificial.

Específicamente, frente al **Desarrollo de programas de concientización y capacitación,** consideramos adecuado que en el Plan Decenal del sistema de justicia, (2017 - 2027) contemple un programa para fortalecer el uso y apropiación de TIC y generar un cambio cultural en el sistema de justicia colombiano alrededor del uso de TIC; sin embargo, estos programas se deben complementar como ya se indicó con los programas de concientización y sensibilización sobre los riesgos cibernéticos, la cultura de la privacidad y protección de la información y los programas de capacitación especializada. Se recomienda la suscripción de convenios entre la Rama Judicial y el Ministerio de las TIC, para que servidores judiciales participen de las convocatorias para participar en los varios programas de maestría en seguridad de la información, seguridad digital y ciberseguridad ofertados por Universidades colombianas; Igualmente, es conveniente el diseño de una estrategia de formación, a través de diplomados, en modalidad presencial o virtual, ofertados por universidades colombianas o extranjeras en tema de ciberseguridad.

Por su parte, para **incrementar la infraestructura para manejar los ciberataques** se destaca que es acertado que el Plan Decenal del sistema de justicia, (2017 - 2027) proponga un objetivo específico para "Generar una política de seguridad de la información y protección de datos", el cual tiene acciones concretas, las cuales podemos relacionar con el marco de ciberseguridad NIST en sus funciones de: Identificar mediante la identificación de los riesgos de la información reservada o sensible necesaria para intercambiar a nivel interinstitucional

e intersectorial, acción que debería estar terminada en 2021; Proteger, a través de la creación de los mecanismos de protección de datos (Ejemplo: encriptación, anonimización, códigos de seguridad, entre otros), el diseño de guías y protocolos para la protección de información e infraestructura vulnerable del sistema de justicia y el análisis de puntos críticos y rutas de acción definidas, que deberían estar terminadas en 2026 y 2027. Detectar, por medio del fortalecimiento a nivel institucional las áreas de tecnología y demás recursos para materializar las políticas de seguridad, junto con la implementación de procedimientos asociados a la ISO 27001, acción que se culminaría en 2023. Recuperar a través de elaborar e implementar los planes de recuperación anti-desastres de la infraestructura TIC acción a culminar en 2026.

Sin embargo, se sugiere complementar el Plan Decenal con acciones relacionadas con: el diseño de lineamientos y protocolos para tener los suficientes controles para garantizar la confianza digital y protección de datos a los servidores judiciales, sujetos procesales y ciudadanía en general tanto en todas las aplicaciones digitales y las herramientas de uso dentro del entorno judicial ya existentes, como en las nuevas aplicaciones que tecnologías emergentes basadas en Inteligencia Artificial el uso de chatbot, o en dispositivos IoT, pueden llegar a demandar; el diseño de mecanismos que permitan reconocer, sobre toda información de los sistemas de justicia digital, quien tiene la titularidad y la autorización del manejo y el uso adecuado de esa información y así determinar el alcance funcional de la misma; y, ; el diseño de una política de transparencia sobre cómo, para qué es tratada y usada la información que se contempla en los procesos judiciales digitales; un plan de pruebas de seguridad para identificar las vulnerabilidades, a través de hackers-buenos y tomar las acciones necesarias

para implementar controles efectivos. La ciberseguridad ha de ser una prioridad en el sistema judicial, en consecuencia, se ha de incrementar la inversión presupuestal para evitar ser vulnerable y resistir a los riesgos cibernéticos.

Por su parte, para **continuar aprendiendo de las experiencias de otros**, es importante recordar que la ciberseguridad es compleja y requiere el compromiso y participación de expertos, por ello se sugiere que las altas cortes, sigan participando del grupo de ejusticia de la cumbre judicial iberoamericana, para ser parte de los diagnósticos, del análisis de brechas y del intercambio de conocimientos que les permita generar sinergias. Sin perjuicio, de establecer otras alianzas que permitan generar y consolidar redes de trabajo intersectorial e interinstitucional que busquen alinear distintos intereses de la política pública con el fin que se consolide un efectivo crecimiento e interés en el entorno digital para beneficio de la administración de justicia desde una propuesta integradora de planes y estrategias que desarrollan construcción normativa y cambios institucionales coordinada. También se recomienda realizar, continuamente, ejercicios como el presentado en este artículo, para estar atento a las tendencias y experiencias que los académicos y los sistemas judiciales comparten.

6. Conclusiones

La importancia de este trabajo consistió en describir de la mejor manera, recomendaciones basadas en la RSL para el cumplimiento de las tareas asignadas en un rol digital, dónde están asociadas conocimientos y habilidades de índole tecnológicos, necesarios para mejorar la ejecución de una función de administración de justicia usando instrumentos y herramientas determinadas; que se adquieren a través del proceso continuo de utilización digital y los

riesgos que la indebida utilización de estas herramientas pueden acarrear.

También es cierto que las herramientas digitales consideradas como conocimientos, habilidades, destrezas y actitudes para que un modelo de gestión sea efectivo debe contar con mucha información, a fin de obtener los perfiles, la evaluación y detectar la necesidad de capacitación. En función de estos aportes se debe contar con un proceso formal para el desarrollo digital adaptado a los objetivos sectoriales que la conforman y a su vez, estén en línea directa con la misión y visión de la organización y política digital de la nación.

Toda aplicación TIC está vinculada a conocimientos específicos de ejecución, de esta manera, se evidencia que este tipo de justicia digital, hace referencia a grupos de prerrequisitos cognitivos, donde el sector las necesita para ser capaz de trabajar en forma adecuada en un área específica y concreta. Lo significativo es que se utilicen en la gestión diaria de las necesidades del sector y de la mejor manera, es por eso clave dentro de una gestión acertada, ya que el manejo de la tecnología está precisando a las instituciones a ser más inteligentes en la medida que los procesos institucionales se simplifiquen y sean más céleres y eficaces haciéndose necesario incrementar el valor de dicho conocimiento en las organizaciones del sector justicia.

En el sector de la justicia no debería ser simplemente implementar las TIC únicamente por el bien que ellas causan. En cambio, es esencial una administración de justicia que le dé relevancia a la tecnología como generador de cambio de consolidación de procesos tangibles y beneficios para el desarrollo de la sociedad que genera progreso y se enfila hacia un proceso para impulsar el Estado Colombiano. Por ello, se requiere seguir investigando en el tema,

darle la respectiva importancia respecto a la estructura organizacional para gestionar el uso e incorporación de TIC, con la debida ciberseguridad en los procesos, y, los criterios para definir dicha estructura. No debe perderse de vista que la inversión en la adquisición, desarrollo, uso y mantenimiento en TIC debe estar acompañada de una estrategia coherente de inversión en talento humano lo suficientemente calificados como para explotarlas debidamente.

El sistema judicial debe proteger la información que maneja en los diferentes procesos judiciales, en la medida en que el uso efectivo de la información dependerá de la pertinencia, accesibilidad, calidad, aprehensibilidad que se disponga, todas las acciones que se realicen en busca de esa protección colaborarán en fomentar la eficacia, eficiencia y confiabilidad de las actuaciones judiciales.

Las recomendaciones señaladas buscan ayudar a mitigar la crisis de confianza que hoy sufre la justicia colombiana, que se puede incrementar con la justicia digital por causa de los riesgos cibernéticos a los que se enfrenta. El llevar a cabo estas recomendaciones puede ser un mecanismo para que los ciudadanos sientan que se les brinda una justicia digital confiable.

7. Referencias

Aaltonen, I., Laarni, J., & Tammela, K. (2015). Envisioning e-Justice for Criminal Justice Chain in Finland. *The Electronic Journal of E-Government*, *13*(1), 55–66. Retrieved from www.ejeg.com

Akın Ünver, H. (2018). Politics of Digital Surveillance, National Security and Privacy. *Cyber Gobernance and Digital Democracy 2018/2*, 1–33. https://doi.org/10.1111/1540

Al Swelmiyeen, I., & Al-Nuemat, A. (2017). Facebook e-court: Online justice for online disputes. *Computer Law and Security Review*, *33*(2), 223–236. https://doi.org/10.1016/j.clsr.2016.11.006

Aletras, N., Tsarapatsanis, D., Preoţiuc-Pietro, D., & Lampos, V. (2016). Predicting judicial decisions of the European court of human rights: A natural language processing perspective. *PeerJ Computer Science*, *2016*(10), 1–19. https://doi.org/10.7717/peerj-cs.93

Álvarez-Casallas, L. (2010). Justicia electrónica. *Revista Digital de Derecho Administrativo*, *4*, 43–56. Retrieved from http://www.cepal.org/SocInfo.

Amoni Reverón, G. A. (2013). El uso de la videoconferencia en cumplimiento del principio de inmediación procesal*. *Revista Ius*, *7*(31), 67–85. https://doi.org/10.35487/rius.v7i31.2013.2

Asamblea Legislativa El Salvador. *Decreto 146 de 2015.* , (2015).

Aspis, A. (2010). Las TICs y el Rol de la Justicia en Latinoamérica. *Derecho & Sociedad*, (35), 327-340. Aubert, B., Babin, G., & Aqallal, H. (2014). Providing an Architecture Framework for Cyberjustice. *Laws*, *3*(4), 721–743. https://doi.org/10.3390/laws3040721

Bachman, L. (2014). How to Take advantage of Courtroom Technology. *Iwitness*, *40*(2), 1–2.

Bailey, J. (2016). INTRODUCTION- Fundamental Values in a Technologized Age of Efficiency-annotated. In K. Benyekhlef, J. Bailey, J. Burkell, & F. Gélinas (Eds.), *eAcces to Justice* (pp. 25–27). Retrieved from https://www.jstor.org/stable/j.ctt5hjk9x.8

Banks, D., Hollywood, J. S., Woods, D., Woodson, P. W., & Johnson, N. J. (2016). Full List of Court Needs. In *Fostering Innovation in the U.S. Court System. Identifying High-Priority Technology and Other Needs for Improving Court Operations and Outcomes* (pp. 101–128). RAND Corporation.

Beauchard, R. (2016). Cyberjustice and International Development: Reducing the Gap Between Promises and Accomplishments. In K. Benyekhlef, J. Bailey, & J. Burkell (Eds.), *eAccess to Justice Book*. Retrieved from https://about.jstor.org/terms

Bellone, E. (2015). *Videoconferencing in the Courts: An Exploratory Study of Videoconferencing Impact on the Attorney-Client Relationship in Massachusetts*. Northeastern University.

Benyekhlef, K. (2018). *A tale of Cyberjustice. A modern approach to technology in the Canadian Justice System.* (K. Benyekhlef, Ed.). Cyberjustice Laboratory.

Bonfanti, M. E. (2018). Enhancing cybersecurity by safeguarding information privacy. The European Union and the implementation of the "data protection by design" approach. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3230833.3233289

Caballero, J., de Gracia, G., & Hammergren, L. (2011). *Buenas Prácticas para la implementación de soluciones tecnológicas en la administración de justicia*. Retrieved from www.acdi-cida.gc.ca

Canivet, G. (2016). POSTSCRIPT: eAccess to Justice-Brief Observations. In K. Benyekhlef, J. Bailey, J. Burkell, & F. Gélinas (Eds.), *eAccess to Justice* (pp. 377–381). Retrieved from https://about.jstor.org/terms

Castell, S. (2018). The future decisions of RoboJudge HHJ Arthur Ian Blockchain: Dread, delight or derision? *Computer Law and Security Review*, *34*(4), 739–753. https://doi.org/10.1016/j.clsr.2018.05.011

Castells, M. (1996). *La era de la información: economía, sociedad y cultura* (Vol. 1). Madrid: Alianza Editorial. Center for Cyber and Homeland Security. (2016). Cybersecurity for State and Local Law Enforcement: A Policy Roadmap to Enhance Capabilities. In *Issue Brief #2016-01*. Washington.

Cerrillo i Martínez, A. (2007). E-justicia: las tecnologías de la información y el conocimiento al servicio de la justicia iberoamericana en el siglo XXI. *IDP: Revista de Internet, Derecho y Política*, *3*(4), 5.

Chatfield, A. T., & Reddick, C. G. (2017). Cybersecurity innovation in government: A case study of U.S. pentagon's vulnerability reward program. *ACM International Conference Proceeding Series*, 64–73. https://doi.org/10.1145/3085228.3085233

Chávez, R. J. Á. (2011). *El Modelo del Sistema de Justicia en Línea y su Expansión a otros Ámbitos de la Jurisdicción*. 197–212.

Clark, J. R. (2017). Federal Support and Guidance in the Establishment of Information Sharing Environments: Mid- Atlantic Regional Information Sharing (MARIS) Case Study. In *Issue Brief # 2017 - 01* (Vol. 01). Center for Cyber & Homeland Securoty. The George Whashingtom University.

Clifford, M., & Kinloch, K. (2008). The use of computer simulation evidence in court. *Computer Law and Security Report*, *24*(2), 169–175. https://doi.org/10.1016/j.clsr.2007.11.002

Comisión Europea. (2010). *E-justice* (Vol. 9).

https://doi.org/10.1558/jsrnc.v4il.24 Congreso de la República de Colombia. *Ley 1564 de 2012.* , (2012).

Consejo Superior de la Judicatura. *Justicia para la Gente. Plan de desarrollo de la Justicia 1995-1998.* , (1994). Consejo Superior de la Judicatura. *Acuerdo No. PSAA14-10161.* , (2014).

Consejo Superior de la Judicatura. *Plan decenal de justicia 2017-2027.* , (2017).

Consejo Superior de la Judicatura. *Plan Sectorial de Desarrollo Rama judicial 2019 – 2022 "Justicia Moderna con Transparencia y equidad."* , (2019).

Contini, F., & Velicogna, M. (2011). Del acceso a la información al acceso a la justicia: diez años de e-justice en Europa. *Revista Sistemas Judiciales- El Rol de Las Nuevas Tecnologías En El Sistema de Justicia*, *9*(16), 30– 47.

Coudert, F., Butin, D., & Le Métayer, D. (2015). Body-worn cameras for police accountability: Opportunities and risks. *Computer Law and Security Review*. https://doi.org/10.1016/j.clsr.2015.09.002

Cukier, M., Maimon, D., & Berthier, R. (2012). A journey towards rigorous cybersecurity experiments: On the application of criminological theories. *ACM International Conference Proceeding Series - Learning from Authoritative Security Experiment Results, LASER 2012*, 25–30. https://doi.org/10.1145/2379616.2379620 Cumbre Judicial Iberoamericana Edición XIX. (2018). *Recomendaciones sobre Ciberseguridad.*

Da Luz Batalha, M. (2013). Government and army policies toward cybernetic security and defense in Brazil. *ACM International Conference Proceeding Series*, 265–266. https://doi.org/10.1145/2479724.2479765

Davis, R., Matelevich-hoang, B. J., Barton, A., Debus-, S., Niedzwiecki, E., Matelevich-Hoang, J., … Niedzwiecki,

E. (2015). *Research on Videoconferencing at Post-Arraignment Release Hearings: Phase I Final Report, Executive Summary*.

Departamento Nacional de Planeación. Política de Seguridad Digital. , Documento CONPES 3854 § (2016). Departamento Nacional de Planeación. Politica Nacional de Confianza y Seguridad Digital. , Documento CONPES

3995 § (2020).

Devoe, D., & Frattaroli, S. (2006). *Videoconferencing in the Courtroom: benefits, concerns, and how to move forward*. Retrieved from http://www.fjc.gov/public/home.nsf/autoframe?openform&url_l=/public/home.nsf/inavgeneral?openpage&url

_r=/pu

Dimensional Research. (2016). *Trends in Security Framework Adoption.*

Donoghue, J. (2017). The Rise of Digital Justice: Courtroom Technology, Public Participation and Access to Justice. *The Modern Law Review*, *80*(6), 995–1025. https://doi.org/10.1111/1468-2230.12053

Duaso-Calés, R. (2011). Justicia electrónica y privacidad: nuevas pistas de reflexión sobre la cuestión de la protección de los datos personales y la publicación de las sentencias judiciales en Internet. In *Buenas Prácticas para la Implementación de Soluciones Tecnológicas en la Administración de Justicia* (pp. 177– 191).

Estevez, E., Fillotrani, P., & Linares Lejarraga, S. (2020). *PROMETEA: Transformando la administración de justicia con herramientas de inteligencia artificial*. https://doi.org/10.18235/0002378

European Union Agency for Network and Information Security. (2017). *ENISA overview of cybersecurity and related terminology*. https://doi.org/10.1088/0953-8984/15/17/332

Ewald, U. (2019). Digital Forensics vs. Due Process: Conflicting Standards or Complementary Approaches? *Proceedings of the Third Central European Cybersecurity Conference*, 28:1--28:2. https://doi.org/10.1145/3360664.3362697

Fabra-i-Abat, P., Battle-Rubio, A., Cerrillo-Martínez, A., Galiano-Barajas, A., Peña-Lopez, I., & Colombo- Vilarrasa, C. (2006). *Estudio comparado la justicia en la sociedad del conocimiento. Retos para los países iberoaméricanos*. Retrieved from https://ictlogy.net/articles/fabra_batlle_cerrillo_galiano_pena- lopez_colombo_-_estudio_ejusticia.pdf

Freire Pimentel, A., Mateus, C. P., & Mendes Saldanha, P. (2017). El proceso judicial electrónico, la seguridad jurídica y violaciones de los derechos fundamentales desde el punto de vista del sistema jurídico brasileño. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, (17), 1–19.

Ganesin, A., Supayah, L., & Jamaludi, I. (2016). An overview of cyber security challenges in developing world. *Kuwait Chapter of Arabian Journal of Business and Management Review*, *6*(4), 11–20.

García Barrera, M. E. (2018). Juzgado sin papel, un paso más en la justicia electrónica. *Revista IUS. Revista Del Instituto de Ciencias de Puebla*, *12*(41), 133–154. Retrieved from http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100133

Gil Botero, E. (2019). Las TIC como logro para una justicia moderna. In *Tecnologías al servicio de la Justicia y el Derecho* (pp. 59–69). Bogotá: Pontificia Universidad Javeriana.

Goodison, S. E., Davis, R. C., & Jackson, B. (2015). Digital Evidence and the U.S. Criminal Justice System Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. In S. E. Goodison, R. C. Davis, & B. Jackson (Eds.), *Digital Evidence and the U.S. Criminal Justice System* (p. https://www.rand.org/content/dam/rand/pubs/technic). RAND Corporation.

Gordon, L., & Garrie, D. (2020). *Cybersecurity & the Courthouse: Safeguarding the Judicial Process*. New York: Wolters Kluwer.

Grupo e-justicia - Cumbre Judicial Iberoamericana. (2018). Recomendaciones sobre Ciberseguridad. In *XIX Edición*. Quito.

Hammergren, L. (2011). La Gobernanza Judicial y el uso de Tecnologias de la Información y la Comunicación. In José Antonio Caballero, C. G. Gracia, & L. Hammergren (Eds.), *Buenas Prácticas para la Implementación de Soluciones Tecnológicas en la Administración de Justicia* (pp. 11–26). Retrieved from http://repositorio.unan.edu.ni/2986/1/5624.pdf

Heeks, R. (2005). e-Government as a Carrier of Context. *Journal of Public Policy*, *25*(1), 51–74. https://doi.org/10.1017/S0143814X05000206

Herbert, S. (2015). Improving access to justice through information and communication technologies - Helpdesk Research Report. In *GSDRC Helpdesk Research Report*. Retrieved from www.gsdrc.org

Hilbert, M. (2012). Toward a Conceptual Framework for ICT for Development: Lessons Learned from the Latin American "Cube Framework." *Information Technologies & International Development2*, *8*(4), 243–259.

Hogeveen, B. (2020). Implementing e-government and digital government capabilities in the Pacific. In B. Hogeveen (Ed.), *ICT for development in the Pacific Islands. An assessment of e-government capabilities in Fiji, Papua NewGuine, Samoa, Soloman Islands, Tonga and Vanuatu*. Australian Strategic Policy Institute.

Hollywood, J. S., Boon, J. E., Silberglitt, R., Chow, B. G., & Jackson, B. A. (2015a). Findings and Recommendations. In *High-Priority Information Technology Needs for Law Enforcement* (pp. 51–64). https://doi.org/10.7249/j.ctt14bs4kz.11

Hollywood, J. S., Boon, J. E., Silberglitt, R., Chow, B. G., & Jackson, B. A. (2015b). Information Technology Needs for Law Enforcement. In *High-Priority Information Technology Needs for Law Enforcement* (pp. 25– 49). https://doi.org/10.7249/j.ctt14bs4kz.10

Hollywood, J. S., Woods, D., Lauland, A., Jackson, B. A., & Silberglitt, R. (2018). Emerging Technology Trends and Their Impact on Criminal. In *Research Brief Rand Corporation*. Retrieved from RAND Corporation website: https://www.jstor.org/stable/resrep17696

Hollywood, J. S., Woods, D., Silberglitt, R., Book, B. A. J., & Jackson, B. A. (2015). Using Future Internet Technologies to Strengthen Criminal Justice. In *Using Future Internet Technologies to Strengthen Criminal Justice* (pp. 1–33). https://doi.org/10.7249/j.ctt19w720j.1

Horan, J., & Maine, S. (2014). Criminal Jury Trials in 2030: A Law Odyssey. *Journal of Law and Society*, *41*(4), 551–575. Retrieved from http://www.innocenceproject.org/Content/

INPEC - Subdirección de Planeación. (2019). *Reporte de Audiencias virtuales. Documento interno de trabajo*. Bogotá.

Jackson, B. A., Banks, D., Hollywood, J. S., Woods, D., Royal, A., Woodson, P. W., & Johnson, N. J. (2016a). Conclusions. In *Fostering Innovation in the U.S. Court System. Identifying High-*

Priority Technology and Other Needs for Improving. RAND Corporation.

Jackson, B. A., Banks, D., Hollywood, J. S., Woods, D., Royal, A., Woodson, P. W., & Johnson, N. J. (2016b). Court Technology and Practice Today. In B. A. Jackson, D. Banks, J. S. Hollywood, D. Woods, A. Royal, P.W. Woodson, & N. J. Johnson (Eds.), *Fostering Innovation in the U.S. Court System. Identifying High- Priority Technology and Other Needs for Improving Court Operations and Outcomes* (pp. 19–43). RAND Corporation.

Jackson, B., Banks, D., Hollywood, J. S., Woods, D., Royal, A., Woodson, P. W., & Johnson, N. J. (2016a). From Courts Today to Courts Tomorrow: Identifying and Prioritizing Innovation Needs in Technology, Policy, and Practice. In B. A. Jackson, D. Banks, J. S. Hollywood, D. Woods, A. Royal, P. W. Woodson, & N. J. Johnson (Eds.), *Fostering Innovation in the U.S. Court System Book Subtitle: Identifying High-Priority Tech* (pp. 45– 69). https://doi.org/10.7249/j.ctt1d41ddx.11

Jackson, B., Banks, D., Hollywood, J. S., Woods, D., Royal, A., Woodson, P. W., & Johnson, N. J. (2016b). The State of the U.S. Court System Today. In B. Jackson, D. Banks, J. S. Hollywood, D. Woods, A. Royal, P. W. Woodson, & N. J. Johnson (Eds.), *Fostering Innovation in the U.S. Court System* (pp. 5–17). RAND Corporation.

Kalemi, E., & Yildirim-yayilgan, S. (2016). Ontologies for Social Media Digital Evidence. *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, *10*(2), 1–7.

Katz, J., & Hilbert, M. (2003). *Building an information society: a Latin American and Caribbean perspective* (First). Retrieved from ECLAC website: http://repositorio.cepal.org/handle/11362/2743

Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering - A systematic literature review. *Information and Software Technology*, Vol. 51, pp. 7–15. https://doi.org/10.1016/j.infsof.2008.09.009

Klaver, M., Luiijf, H., Nieuwenhuijs, A., & Al, E. (2011). *RECIPE Good Practices Manual for CIP Policies. For policiy makers in Europe*. Retrieved from https://www.tno.nl/recipereport/

Kramer, F. D., & Butler, R. J. (2019). *A roadmap to better cybersecurity. Changing the model.* Atlantic Council.

Landwehr, C., Boneh, D., Mitchell, J. C., Bellovin, S. M., Landau, S., & Lesk, M. E. (2012). Privacy and cybersecurity: The next 100 years. *Proceedings of the IEEE*, *100*(SPL CONTENT), 1659–1673. https://doi.org/10.1109/JPROC.2012.2189794

Lanier, M. M., & Cooper, A. T. (2016). From papyrus to cyber: how technology has directed law enforcement policy and practice. *Criminal Justice Studies*, *29*(2), 92–104. https://doi.org/10.1080/1478601X.2016.1170280

Li, C., Sheng, Y., Ge, J., & Luo, B. (2019). Apply event extraction techniques to the judicial field. *UbiComp/ISWC2019- Adjunct Proceedings of the 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2019 ACM International Symposium on Wearable Computers*, 492–497. https://doi.org/10.1145/3341162.3345608

Lillo Lobos, R. (2011). El Uso de Nuevas Tecnologías en el Sistema Judicial: experiencias y precauciones 1. In José A; Caballero, C. G. de Grácia, & L. Hammergren (Eds.), *Buenas Prácticas para la Implementación de Soluciones Tecnológicas en la Administración de Justicia* (pp. 117–140). Retrieved from http://www.cejamericas.

Londoño-Sepulveda, R. N. (2010). The use of ICT in judicial procedures: a proposal for online justice L'usage des TIC dans les procédures judiciaires: une proposition de la justice en ligne. *Revista Facultad de Derecho y Ciencias Políticas*, *40*(112), 123–142.

López-Jaramillo, G. S. (2019). Nuevo modelo de justicia en línea colombiano. In *Tecnologías al servicio de la Justicia y el Derecho* (pp. 37–58). Bogotá: Pontificia Universidad Javeriana.

Maestropiedra, N. (2012). Carga de datos contextuales para el análisis y gestión del proceso judicial. *Simposio Argentino de Informática y Derecho*, 47–56.

Mania, K. (2015). Online dispute resolution: The future of justice. *International Comparative Jurisprudence*, *1*(1), 76–86. https://doi.org/10.1016/j.icj.2015.10.006

Martin Katz, D., Bommarito, M. J., & Blackman, J. (2017). A general approach for predicting the behavior of the Supreme Court of the United States. *PLoS ONE*, *12*(4), 1–18. https://doi.org/10.1371/journal.pone.0174698

Mclaughlin, B. J. (2018). Cybersecurity: Protecting Court Data Assets *. In *Trends in State Courts* (pp. 67–72).

Mcmillion, R. (2013). It's Not Just the Economy: The 113th Congress will face a full agenda of issues relating to the justice system. *ABA Journal*, *99*, 62. Retrieved from https://about.jstor.org/terms

Ministerio de las Tecnologías de la información y comunicaciones de Colombia. (2008). *Plan Nacional de Tecnologías de la Información y las Comunicaciones. 2008-2019*. 165.

Morales-Navarro, K. (2011). La inclusión de las tecnologías en la gestión judicial Poder Judicial de República de Costa Rica. In C. Riego & A. Binder (Eds.), *El rol de las Nuevas Tecnologías en el Sistema de Justicia* (pp. 48–55).

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity*.

Norris Rodin, D., & Rodin, D. N. (2015). The Cybersecurity Partnership : A Proposal For Cyberthreat Information Sharing Between Contractors And The Federal Government. *Public Contract Law Journal*, *44*(3), 505–528. https://doi.org/10.2307/26419479

NU., GK., GS., RamasubramanianK., & S. K. (2020). The LAWBO: A Smart Lawyer Chatbot: AI Assisted System to scan past judgement to recommend appropriate IPC rules for case preparation. *Probyto Journal of AI Research*, *1*(1).

Palmgren, K. (2018). The use of Online Dispute Resolution: How to best integrate an online Court into the Victorian Public Justice System. In *CHURCHILL FELLOWSHIP REPORT*.

Pijnenburg-Muller, L. (2015). Cyber Security Capacity Building in Developing Countries. In *Policy Brief*. Retrieved from http://www.iss.europa.eu/activities/detail/article/cyber-ca-

Pontificia Universidad Javeriana, Rincón Martínez, L. M., Apperson, J. A., López Jaramillo, G. S., Gil Botero, E., Rincón Cárdenas, E., … Álvarez Londoño, L. F. S. J. 1947-. (2019). *Tecnologías al servicio de la Justicia y el derecho*. Bogotá: Pontificia Universidad Javeriana.

Presidencia de la República de Colombia. *Decreto 806 de 2020.* , (2020).

Prins, C. (2018). Digital justice. *Computer Law and Security Review*, *34*(4), 920–923. https://doi.org/10.1016/j.clsr.2018.05.024

Quispe Angulo, C. (2018). *El expediente digital y su incidencia en la administración de justicia en el Perú* (Universidad Señor de Sipán). Retrieved from http://repositorio.uss.edu.pe/bitstream/handle/uss/5100/Quispe Angulo%2C Carlos Alberto.pdf?sequence=1&isAllowed=y

Rico-Pinto, J., & Sánchez-Torres, J. M. (2019). Characterization of G2G Interoperability Factors. *ECDG 2019 19th European Conference on Digital Government*, 107–115. Nothern Cyprus: Academic Conferences International Limited.

Rincón-Cárdenas, E. (2013). *Tecnología y Administración de Justicia en Colombia*. Retrieved from www.colombiadigital.net

Rincón-Cárdenas, E. (2019). Justicia y TICs, desde el Plan Nacional de TIC, Articulación de una Política Pública. In *Tecnologías al servicio de la Justicia y el Derecho*.

Ríos Ruiz, A. de los A. (2017). *La Justicia electrónica en México: Visión comparada con América Latina*.

Rojas Quispe, T. (2014). La notificación virtual y su implementación en la Administración de Justicia en el Perú. *Revista Científica Jurídica SSIAS. Investigación Jurídica*, *7*(1), 1–19.

Rosa, J., Teixeira, C., & Sousa Pinto, J. (2013). Risk factors in e-justice information systems. *Government Information Quarterly*, *30*(3), 241–256. https://doi.org/10.1016/j.giq.2013.02.002

Sánchez-Acevedo, M. E. (2017). *Estrategia jurídica para la gestión, análisis y ciberseguridad de la información en la investigación penal*.

Sánchez-Torres, J. M. (1998). *Diseño de la metodología para la evaluación del impacto de la implementación de las TIC en la Rama Judicial Colombiana.* Universidad Nacional de Colombia.

Sánchez-Torres, J. M. (2005). *Propuesta metodologica para evaluar las politicas publicas de promocion del e- government como campo de aplicacion de la Sociedad de la Informacion .Conceptualizacion y aplicacion empirica en el caso colombiano*. Universidad Autónoma de Madrid.

Sánchez-Torres, J. M. (2017). *Vigilancia Tecnológica e Inteligencia Competitiva en la práctica. Guía de*

aplicación. Bogotá.

Sánchez-Torres, J. M., González-Zabala, M. P., & Sánchez-Muñoz, M. P. (2012). La Sociedad de la Información: Génesis, Iniciativas, Concepto y su Relación con las TIC. *UIS Ingenierías - Revista de La Facultad de Ingenierías Físico Mecánicas*, *11*(1), 113–128.

Stockman, M. (2014). Insider hacking: Applying situational crime prevention to a new white-collar crime. *RIIT 2014 - Proceedings of the 3rd Annual Conference on Research in Information Technology*, 53–56. https://doi.org/10.1145/2656434.2656436

Şulea, O. M., Zampieri, M., Vela, M., & Van Genabith, J. (2017). Predicting the law area and decisions of French supreme court cases. *International Conference Recent Advances in Natural Language Processing, RANLP*, *2017-Septe*, 716–722. https://doi.org/10.26615/978-954-452-049-6-092

Susskind, R. (2019). *Online Courts and the Future of Justice*. Oxford: Oxford University Press.

The International Organization for Standardization. (2012). ISO/IEC 27032:2012 Information Technology — Security Techniques — Guidelines for Cybersecurity. *ISO.Org [Online]*.

Toapanta, S. M. T., Gurumendi, A. J., & Gallegos, L. E. M. (2019). An approach of national and international cybersecurity laws and standards to mitigate information risks in public organizations of Ecuador. *ACM International Conference Proceeding Series ICETEM 2019*, 61–66. https://doi.org/10.1145/3375900.3375909

Tomlinson, J. (2019). How digital administrative justice is made. *Justice in the Digital State*, 63–88. https://doi.org/10.2307/j.ctvndv808.10

Treglia, J. V., & Park, J. S. (2009). Towards trusted intelligence information sharing. *Proceedings of the ACM SIGKDD Workshop on CyberSecurity and Intelligence Informatics, CSI-KDD in Conjunction with SIGKDD'09*, 45–52. https://doi.org/10.1145/1599272.1599283

UIT, U. I. de T. (2008). UIT-T X.1205 Aspectos generales de la ciberseguridad. *Sector De Normalización De Las Telecomunicaciones De La Uit*, *1205*.

Velicogna, M. (2017). In Search of Smartness: The EU e-Justice Challenge. *Informatics*, *4*(4), 38. https://doi.org/10.3390/informatics4040038

Vermeys, N. (2016). Privacy v. Transparency: How Remote Access to Court Records Forces Us to Re-examine Our Fundamental Values. In K. Benyekhlef, J. Bailey, J. Burkell, & F. Gélinas (Eds.), *eAccess to Justice*.
Retrieved from https://about.jstor.org/terms

Vermeys, N., & Acevedo-Lanas, M. (2020). L'émergence et l'évolution des tribunaux virtuels au Canada – L'exemple de la Plateforme d'aide au règlement des litiges en ligne (PARLe). *Revue Juridique de La Sorbonne*, *1*, 22–51. Retrieved from https://www.lawsitesblog.com/2016/04/future-online-dispute- resolution.html.

Vermeys, N. W., & Benyekhlef, K. (2011). Best Practices in the Field of Cyberjustice. In José A; Caballero, C. G. de Grácia, & L. Hammergren (Eds.), *Buenas Prácticas para la Implementación de Soluciones Tecnológicas en la Administración de Justicia*. Retrieved from IIJusticia website: http://www.cyberjusticelaboratory.org.

Weinstock, D. (2016). Cyberjustice and Ethical Perspectives of Procedural law Chapter. In K. Benyekhlef, J. Bailey, J. Burkell, & F. Gélinas (Eds.), *eAccess to Justice* (pp. 305–315). Univeristy of Ottawa Press.

Westermann, H., Walker, V. R., Ashley, K. D., & Benyekhlef, K. (2019). Using factors to predict and analyze landlord-tenant decisions to increase access to Justice. *Proceedings of the 17th International Conference on Artificial Intelligence and Law, ICAIL 2019*, 133–142. https://doi.org/10.1145/3322640.3326732

Zimmerman, C. (2013). *An Evaluation of Private-Sector Digital Forensics Processes and Practices* (City University of New York). Retrieved from http://icacci-conference.org