LA CONSTRUCCIÓN DE LA CIBERSEGURIDAD EN EL ESTADO COLOMBIANO: UN ENFOQUE DESDE EL DERECHO ADMINISTRATIVO.

THE CONSTRUCTION OF CYBERSECURITY IN THE COLOMBIAN STATE: AN ADMINISTRATIVE LAW APPROACH.

Walter Rodríguez Henao[1]

Leidy Johana Morales Buriticá[2]

Julián Mauricio Cadavid Restrepo[3]

Institución Universitaria de Envigado

Especialización en Derecho Administrativo

Año 2023

[1] Abogado. Estudiante de Especialización en Derecho Administrativo en la Institución Universitaria de Envigado. Correo: wrodriguez@correo.iue.edu.co

[2] Abogada. Estudiante de Especialización en Derecho Administrativo en la Institución Universitaria de Envigado. Correo: ljmorales@correo.iue.edu.co

[3] Abogado. Estudiante de Especialización en Derecho Administrativo en la Institución Universitaria de Envigado. Correo: jmcadavid@correo.iue.edu.co

RESUMEN

El artículo aborda la crítica importancia de la ciberseguridad en la sociedad contemporánea, particularmente en el contexto colombiano. Se enfoca en la perspectiva del Derecho Administrativo y su relación con la consolidación del gobierno digital como factor clave en la discusión. Se desglosan tres ejes temáticos: primero, cómo la ciberseguridad se integra en el marco del Derecho Administrativo en Colombia y los desafíos que enfrenta la administración pública en la implementación de políticas de ciberseguridad. Segundo, se analiza la construcción de políticas públicas digitales desde la perspectiva del buen gobierno. Finalmente, se profundiza en la efectividad de la administración pública en la prevención de delitos cibernéticos, destacando la evolución tecnológica y su influencia en estos delitos.

Palabras clave: Ciberseguridad, gobierno digital, políticas públicas, buen gobierno, derecho administrativo.

ABSTRACT

The article addresses the critical importance of cybersecurity in contemporary society, particularly in the Colombian context. It focuses on the perspective of Administrative Law and its relationship with the consolidation of digital government as a key factor in the discussion. It breaks down three fundamental thematic axes: first, how cybersecurity is integrated into the framework of Administrative Law in Colombia and the challenges faced by the public administration in the implementation of cybersecurity policies. Second, it analyzes the construction of digital public policies from the perspective of good governance, with case studies of the European Union and Colombia. Finally, it delves into the effectiveness of public administration in the prevention of cybercrime, highlighting the technological evolution and its influence on these crimes.

Key words: Cybersecurity, digital government, public policy, good governance, administrative law.

INTRODUCCIÓN

La ciberseguridad se ha convertido en un tema de importancia crítica en la sociedad contemporánea, donde la tecnología desempeña un papel central en todas las esferas de la vida. En el contexto colombiano, la ciberseguridad puede ser abordada desde perspectiva del Derecho Administrativo, considerando la consolidación del gobierno digital como uno de los principales motores de esta discusión. Este artículo se sumerge en un análisis profundo y multidimensional de la ciberseguridad en el Estado colombiano, examinando su desarrollo desde el Derecho Administrativo y explorando sus conexiones con la consolidación del gobierno digital.

Para comprender el panorama actual, se abordan tres ejes temáticos clave en este artículo. En primer lugar, se analiza cómo la ciberseguridad se integra en el marco del Derecho Administrativo en Colombia en el contexto de la consolidación del gobierno digital. Se exploran las leyes y regulaciones pertinentes, así como los desafíos que enfrenta la administración pública en la implementación de políticas de ciberseguridad efectivas.

En segundo lugar, se examina la construcción de una política pública digital desde la perspectiva del buen gobierno, centrándose en dos casos de estudio: la Unión Europea y Colombia. Se investiga cómo estas regiones han abordado la modernización de la administración pública a través de estrategias digitales, incluyendo la promoción de la transparencia, la participación ciudadana y la cooperación interinstitucional.

Finalmente, se analiza la efectividad de la administración pública en la prevención de delitos cibernéticos, tales como, Ataques de denegación de servicio, virus espías, captura de información u otro tipo de delitos cometidos en el ciberespacio y que pueden afectar el debido funcionamiento de la administración pública. Se profundiza en la evolución tecnológica y sus implicaciones sociales en la aparición y propagación de ciberdelitos, destacando la importancia de la colaboración internacional y la sensibilización pública en la lucha contra estas amenazas. Por lo que, este artículo busca arrojar luz sobre el complejo panorama de la ciberseguridad en el Estado colombiano, destacando su relación con el Derecho Administrativo, la consolidación del gobierno digital y los desafíos actuales en la prevención de delitos cibernéticos.

Mediante una metodología cualitativa, bajo un enfoque analítico- descriptivo, se espera proporcionar una visión integral de un tema crucial en la sociedad moderna.

1. La ciberseguridad desde el derecho Administrativo en Colombia: Análisis a partir de la consolidación del gobierno digital.

El gobierno digital, según Fernández Valenzuela, Fernández Ocaña, Hidalgo Soto, Aliaga Cotrina, & Fuster-Guillén (2023), se define como la utilización de tecnologías de la información y la comunicación (TIC) para modernizar la prestación de servicios gubernamentales, la toma de decisiones y la interacción con los ciudadanos. Esta estrategia implica la digitalización de procesos administrativos y la implementación de servicios en línea, incluyendo la recopilación y análisis de datos. El propósito es fomentar la participación ciudadana mediante acciones que faciliten el acceso a las instituciones estatales desde el ciberespacio y plataformas digitales. Esto, a su vez, mejora la eficiencia, transparencia y accesibilidad de la administración pública, fortaleciendo aspectos clave de un buen gobierno al proporcionar a los ciudadanos un acceso más rápido y conveniente a información y servicios gubernamentales.

El gobierno digital, al basarse en tecnologías de la información, expone vulnerabilidades a la privacidad, destacando la importancia de la ciberseguridad. En este contexto, la creciente dependencia estatal de las TIC aumenta las amenazas cibernéticas. Desde la perspectiva del derecho administrativo en Colombia, es esencial analizar cómo se aborda la ciberseguridad en este entorno, destacando su prioridad en la consolidación del gobierno digital.

Según Pirni, Giampellegrini, & Raffini (2019), el establecimiento de una ciberseguridad efectiva se ha vuelto crucial a partir del marco legal y regulatorio. Las leyes y decretos sobre protección de datos, gestión de incidentes cibernéticos y la responsabilidad estatal en la prevención de amenazas digitales son aspectos fundamentales. La constante revisión y actualización de estas normativas son retos para garantizar la seguridad en el gobierno digital. Es responsabilidad del Estado construir un modelo de seguridad eficiente en el ciberespacio, protegiendo los derechos de los

ciudadanos y resguardando las instituciones públicas. Esto se puede lograr a través de la colaboración armónica y otros principios rectores en la Administración pública (Jiménez Vargas & Calle Villegas, 2015).

En ese sentido, (Jara Fuentealba & Jorquera Cruz, 2021) da a entender como en la era digital es necesario por parte del Estado que este se adapte a las nuevas prácticas sociales; por tanto, el análisis desde el derecho administrativo en Colombia nos permite comprender cómo el Estado se adapta a un entorno cada vez más digitalizado.

En el ámbito del derecho administrativo en Colombia, la ciberseguridad implica salvaguardar la privacidad y datos personales en el gobierno digital. Esto requiere medidas de seguridad robustas y políticas de privacidad alineadas con las leyes vigentes. La evaluación de la efectividad de las estrategias de ciberseguridad plantea preguntas cruciales: ¿Se logran los objetivos de protección de datos y prevención de amenazas cibernéticas en el gobierno digital colombiano? ¿Existen mecanismos de supervisión y rendición de cuentas para asegurar que el Estado cumple con sus responsabilidades en ciberseguridad?

1.1. El gobierno digital y su desarrollo normativo en Colombia.

La Ley 1341 de 2009, conocida como la Ley de Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, establece las bases para políticas y estrategias en el gobierno digital. La Ley 1712 de 2014 fortalece la transparencia gubernamental. Este marco normativo abarca ciberseguridad y protección de datos, evidenciado en la Ley 1581 de 2012. Aunque Colombia impulsa la transformación digital estatal, persisten vacíos en la administración pública, desactualizada ante nuevas tecnologías y dinámicas sociales.

El gobierno digital en Colombia ha experimentado un crecimiento notable respaldado por un desarrollo normativo que ha buscado ser sólido, no obstante, frente a las nuevas dinámicas tecnológicas se ha quedado corto de capacidad de acción. Las leyes y regulaciones en este campo buscan promover la modernización de la

administración pública, garantizar la transparencia y el acceso a la información, y proteger la seguridad de los datos en un entorno digital en constante evolución.

El marco legal colombiano está actualizándose para fortalecer la capacidad estatal frente a las nuevas tecnologías, evidenciado en normativas como la Ley 1581 de 2012, Ley 1273 de 2009, Decreto 338 de 2022 y CONPES 3650 de 2010. Más allá de establecer el gobierno digital, el Estado busca consolidar una infraestructura cibernética eficiente para mejorar la comunicación con las comunidades, abordar problemas territoriales y salvaguardar derechos fundamentales ante las amenazas de las nuevas tecnologías. A continuación, se presenta una tabla para explicar la relación del gobierno digital desde el derecho interno.

Tabla 1. Ordenamiento jurídico colombiano en materia de nuevas tecnologías: Acercamiento a partir del Gobierno digital.

Ley o Decreto	**En qué consiste**	**Relación con el gobierno digital**
Ley 1581 de 2012	Se establecen disposiciones generales en materia de protección de datos personales y privacidad.	El gobierno digital necesita una política de protección de datos para garantizar el derecho a la intimidad de las personas.
Ley 1273 de 2009	Establece tipos penales relacionados a seguridad digital, ciberdelitos, y demás vulneraciones al bien jurídico tutelado desde el ciberespacio.	El gobierno digital debe estar a la vanguardia y preparado para abordar problemas que puedan surgir con nuevas tecnologías.

Decreto 338 de 2022	Desde este Decreto se crean las siguientes dependencias: • Consejo Nacional de Seguridad Digital. • Centro Nacional de Coordinación y Respuesta a Incidentes de Seguridad Digital. Estas dependencias establecen pautas para la infraestructura cibernética, incluyendo riesgos y respuestas a incidentes.	El decreto demuestra el compromiso del Estado con el ciberespacio y su capacidad de respuesta a las nuevas tecnologías en la era digital.
CONPES 3650 de 2010	Se declara la importancia estratégica de la Agenda de Conectividad, que busca masificar el uso de TIC en las instituciones del Estado y modernizar su infraestructura tecnológica.	La agenda de gobierno digital busca hacer que el Estado sea accesible para todos, y este CONPES establece la meta de modernizar la tecnología en todas las instituciones gubernamentales.
CONPES 3854 de 2016	Crea una política nacional para fortalecer la capacidad del Estado en seguridad digital, incluyendo la	Después de implementar el gobierno digital, se necesitan políticas de ciberseguridad para proteger la privacidad y los derechos

	identificación y mitigación de riesgos cibernéticos.	fundamentales de los usuarios de las plataformas gubernamentales.
CONPES 3975 de 2019	A partir del CONPES 3975. El Estado busca potenciar la generación de valor social y económico a través de la transformación digital y la accesibilidad a la información, impulsando la productividad en la 4ª Revolución Industrial.	Tras lo mencionado, el Estado necesita una agenda de transformación digital para adaptarse a los cambios constantes en las nuevas tecnologías

Fuente: Desarrollo propio.

Colombia ha desarrollado un marco normativo específico para el gobierno digital a nivel municipal y departamental, permitiendo una adaptación descentralizada a las necesidades regionales. La creación de normativas y planes estratégicos locales ha fortalecido la implementación de soluciones tecnológicas en la administración pública regional.

Podemos ver como Ferriz Sánchez (2022) nos indica que es importante destacar que el desarrollo normativo en el gobierno digital es un proceso dinámico que continúa evolucionando para abordar los desafíos cambiantes de la era digital. La adaptación a las tendencias tecnológicas emergentes, como la inteligencia artificial y la automatización, requerirá una revisión constante de las regulaciones existentes para garantizar que sigan siendo relevantes y efectivas en la promoción de una administración pública eficiente y orientada hacia el ciudadano en Colombia.

1.2. Desafíos de la administración pública en la consolidación del gobierno digital: Un acercamiento a partir del Derecho administrativo.

La consolidación del gobierno digital en la administración pública plantea una serie de desafíos que merecen un análisis detenido desde la perspectiva del Derecho administrativo. Uno de los desafíos clave es la adaptación de la regulación legal existente a un entorno digital en constante evolución. Las leyes y regulaciones que gobiernan la administración pública deben ser revisadas y actualizadas para abordar temas como la ciberseguridad, la protección de datos y la interoperabilidad de sistemas en el contexto del gobierno digital.

De esta forma, se evidencia otro desafío importante, el cual radica en garantizar la transparencia y la rendición de cuentas en un entorno digital. La administración pública entonces debe encontrar formas de mantener la integridad y la confidencialidad de la información. Ello, al tiempo que permite un acceso público eficiente y controlado. Esta situación, no implica únicamente la implementación de medidas tecnológicas adecuadas, por el contrario, también la promulgación de normativas que regulen la gestión de datos y la transparencia en línea.

La formación del personal en la administración pública es crucial para abordar los desafíos del gobierno digital. La adopción de nuevas tecnologías y la comprensión de cambios legales y técnicos son esenciales para que los funcionarios públicos sean efectivos en un entorno digital. Asegurar la participación ciudadana efectiva es otro reto, requiriendo acceso a servicios en línea y políticas que fomenten la inclusión digital y accesibilidad para todos, independientemente de sus habilidades tecnológicas.

Según, (Alegre Rodríguez & Padilla López, 2023) se evidencian de igual forma desafíos importantes, tal y como es la gestión eficiente de la información en un entorno digital. La administración pública maneja una gran cantidad de datos, y la migración hacia un gobierno digital implica la digitalización y el almacenamiento seguro de esta información. Esto plantea preguntas sobre la propiedad, el acceso y la protección de estos datos, lo que requiere una regulación adecuada y la implementación de estándares de seguridad de la información.

Tras comprender entonces aquella correlación entre las nuevas tecnologías en materia de Gobierno digital, y Derecho, es posible identificar aquel papel que desempeña el Estado en la superación de estos desafíos en la consolidación de un gobierno abierto en Colombia. La revisión y actualización constante de las regulaciones, el fomento de la transparencia y la participación ciudadana, así como la gestión eficiente de datos, son elementos cruciales para lograr una administración pública digital efectiva y que responda a las necesidades cambiantes de la sociedad.

2. La construcción de una política pública digital: Un acercamiento a partir del buen gobierno.

La construcción de una política pública digital es un proceso fundamental en la era moderna, donde la tecnología desempeña un papel central en la vida de las sociedades. Desde la perspectiva del buen gobierno, este enfoque se convierte en un componente esencial para garantizar la eficiencia, la transparencia y la participación ciudadana en la gestión pública. Una política pública digital efectiva no solo se centra en la implementación de tecnologías, sino que también abarca la formulación de estrategias que respondan a las necesidades de la población.

El proceso de construcción de una política pública digital, según (Sarmiento Loaiza, 2023) debe involucrar a diversos actores, desde funcionarios gubernamentales hasta la sociedad civil y el sector privado. La colaboración y la consulta son esenciales para identificar las áreas clave donde la tecnología puede mejorar los servicios públicos y optimizar la toma de decisiones. Además, es fundamental establecer un marco normativo que respalde la implementación de la política digital y que garantice la protección de datos y la ciberseguridad.

El enfoque en el buen gobierno implica que una política pública digital debe estar alineada con los principios de responsabilidad, transparencia y participación. Esto, según (Solé Ponce, 2023) implica la rendición de cuentas en la gestión de recursos públicos digitales, la disponibilidad de información para los ciudadanos y la promoción de mecanismos de participación que permitan a la sociedad influir en la formulación y evaluación de políticas digitales. Es así como, es factible identificar cómo a partir de la

construcción de una política pública digital desde la perspectiva del buen gobierno es un proceso integral que busca aprovechar la tecnología para mejorar la gestión pública y fortalecer la democracia. La colaboración, la normativa adecuada y el enfoque en la responsabilidad y la transparencia son fundamentales para asegurar que estas políticas cumplan con los objetivos de mejorar la calidad de vida de los ciudadanos y promover un gobierno más eficiente y participativo.

Un elemento esencial en la construcción de una política pública digital es la evaluación continua de su impacto y eficacia. El buen gobierno, entonces, requiere que las políticas digitales se sometan a un escrutinio constante para determinar si están cumpliendo sus objetivos y si se están utilizando de manera eficiente los recursos públicos (Ferriz Sánchez, 2022). Esto implica la recolección y el análisis de datos para medir el rendimiento y la satisfacción del usuario, lo que a su vez permite ajustar y mejorar las estrategias en función de los resultados obtenidos.

La elaboración de una política pública digital debe priorizar la accesibilidad e inclusión digital. Para asegurar que todos los ciudadanos se beneficien del gobierno digital, es esencial abordar las brechas digitales en la sociedad, implementando medidas específicas para incluir a grupos marginados o con acceso limitado a la tecnología. En este contexto, el gobierno digital contribuye a consolidar un estado garante, basándose en principios rectores como el pluralismo jurídico y derechos universales como el buen gobierno. Esto se traduce en políticas públicas que mejoran la accesibilidad a las instituciones y dependencias estatales a través de las nuevas tecnologías.

Así las cosas, entre las diferentes estrategias a implementar por parte del Estado para promover el gobierno digital y su accesibilidad, está la digitalización de servicios gubernamentales, la cual surtirá efecto de manera transitoria, transformando trámites y procesos en línea para facilitar su acceso desde cualquier lugar y dispositivo, sin que ello implique vulnerabilidades a la información personal de quienes hagan uso de estas herramientas. Además, se deben desarrollar plataformas intuitivas y accesibles que cumplan con estándares de facilidad y accesibilidad web, garantizando que personas con discapacidades puedan utilizarlos sin dificultad.

Es así como, a través de la capacitación y sensibilización de empleados públicos y ciudadanos, se puede fomentar el uso y acceso de herramientas esenciales para acceder al Estado y todos los servicios que este presta y oferta a la comunidad en la era digital. Asimismo, desde la promoción de canales de comunicación bidireccionales para recibir retroalimentación y mejorar continuamente. Todo ello, según resalta (Figueroa G., 2013), debe estar adecuado a una política idónea en materia de seguridad de datos y la privacidad, por ende, deben ser prioritarias para generar confianza en los usuarios. En conjunto, estas estrategias pueden crear un gobierno digital más inclusivo y accesible para todos los ciudadanos.

En síntesis, una política pública digital efectiva es un componente esencial del buen gobierno en la era digital. Al promover la eficiencia, la transparencia y la participación ciudadana, estas políticas contribuyen a fortalecer la confianza en las instituciones gubernamentales y a mejorar la calidad de vida de los ciudadanos. La construcción y el mantenimiento de estas políticas deben ser un esfuerzo continuo y colaborativo que se adapte a las cambiantes necesidades y expectativas de la sociedad en la era digital.

3. La efectividad de la administración pública en la prevención de delitos cibernéticos.

La efectividad de la administración pública en la prevención de delitos cibernéticos es un tema crítico en la era digital actual, (Chávez Ramos, 2018) expone que, las amenazas cibernéticas representan un riesgo creciente tanto para los gobiernos como para los ciudadanos. En este contexto, es esencial que la administración pública juegue un papel activo en la prevención y mitigación de estos delitos.

La administración pública debe estar equipada con las herramientas y los recursos adecuados para identificar y abordar las amenazas cibernéticas de manera proactiva. Esto incluye la inversión en tecnología de vanguardia, así como la capacitación continua del personal en materia de ciberseguridad. La creación de equipos especializados y la colaboración con expertos en seguridad cibernética pueden fortalecer aún más las capacidades del gobierno en este campo. Asimismo, (Pirni,

Giampellegrini, & Raffini, 2019) recalca que, la cooperación entre diferentes entidades gubernamentales y la coordinación a nivel nacional e internacional son aspectos clave para combatir eficazmente los delitos cibernéticos. Los delincuentes cibernéticos a menudo operan más allá de las fronteras, por lo que la colaboración internacional es esencial para rastrear y enjuiciar a los responsables. De esta forma, los acuerdos de intercambio de información y la participación en organismos internacionales de ciberseguridad pueden mejorar la efectividad de la administración pública en la prevención de delitos cibernéticos.

Por ende, la concienciación y la educación de los ciudadanos son fundamentales para prevenir los delitos cibernéticos. La administración pública puede desempeñar un papel importante en la promoción de prácticas de seguridad cibernética entre la población. Esto incluye la difusión de información sobre amenazas cibernéticas, la promoción de contraseñas seguras y la concienciación sobre estafas en línea.

En ese sentido, es factible denotar que, la efectividad de la administración pública en la prevención de delitos cibernéticos depende de una combinación de recursos, capacitación, cooperación y educación. (Solé Ponce, 2023) En un mundo digital cada vez más interconectado, la capacidad del gobierno para proteger a sus ciudadanos y sus activos digitales es crucial. La prevención de delitos cibernéticos es un desafío constante que requiere una respuesta proactiva y coordinada de la administración pública.

La eficacia de la administración pública en prevenir delitos cibernéticos se relaciona con la implementación de políticas y regulaciones adecuadas. Según (Pons Gamón, 2017), es crucial establecer marcos legales claros y actualizados que definan con precisión los delitos cibernéticos y sus sanciones, alineándolos con estándares internacionales y adaptándolos a las cambiantes amenazas cibernéticas. De acuerdo con (Hamdi et al., 2021), los estándares internacionales ideales en ciberseguridad deben ser flexibles y actualizarse continuamente para hacer frente a las tácticas cambiantes de actores maliciosos. Este enfoque coincide con las recomendaciones del buen gobierno, según (Ferriz Sánchez, 2022), que abogan por estándares respaldados por una

comunidad global de expertos en seguridad cibernética, proporcionando claridad y actualización para guiar la implementación de medidas de seguridad efectivas por parte de organizaciones y gobiernos.

La cooperación con el sector privado y la sociedad civil es otro aspecto fundamental. Entendiendo que, muchas infraestructuras críticas y datos sensibles están en manos del sector privado; así las cosas (Toscano, 2017) indica cómo, por lo que la colaboración con empresas y organizaciones no gubernamentales es esencial para fortalecer la seguridad cibernética en general. La administración pública debe establecer mecanismos de intercambio de información y trabajo conjunto con el sector privado para detectar y mitigar amenazas de manera efectiva. Además, la administración pública debe estar preparada para responder de manera rápida y eficaz a incidentes cibernéticos. Esto implica contar con planes de respuesta a incidentes y equipos de ciberseguridad bien entrenados que puedan actuar de inmediato para contener y mitigar los daños cuando ocurra un ataque. La coordinación entre diferentes agencias gubernamentales y la comunicación transparente con el público son esenciales en estos casos.

En resumen, la administración pública enfrenta un desafío en constante evolución para prevenir delitos cibernéticos, dado el dinamismo y constante cambio en la ciberseguridad. Es esencial que se mantenga actualizada y adapte sus estrategias para proteger a los ciudadanos y la infraestructura crítica en un entorno cibernético en constante cambio. Alegre Rodríguez & Padilla López (2023) sugieren la implementación de medidas proactivas, inversión en tecnologías avanzadas y colaboración con expertos en ciberseguridad a nivel nacional e internacional. Además, se destaca la importancia de fomentar la conciencia y educación en ciberseguridad, tanto entre empleados públicos como ciudadanos, y desarrollar planes de respuesta a incidentes para abordar rápidamente las amenazas emergentes. En este mundo interconectado y digital, la ciberseguridad se convierte en un pilar fundamental para preservar la integridad de las operaciones gubernamentales y proteger los intereses de la sociedad

3.1. Los ciberdelitos, la evolución tecnológica y sus implicaciones sociales: Análisis a partir de las nuevas tecnologías y las transformaciones sociales.

Los ciberdelitos representan una preocupación creciente en la era digital y están estrechamente relacionados con la evolución tecnológica y sus implicaciones sociales. A medida que la tecnología avanza, los delincuentes cibernéticos encuentran nuevas oportunidades para cometer actos ilícitos en línea. Esta evolución tecnológica ha dado lugar a una amplia variedad de ciberdelitos, que van desde el robo de datos personales y financieros hasta el ciber sabotaje y la difusión de desinformación.

La expansión de las redes sociales y la interconexión global también ha tenido un impacto significativo en la propagación de ciberdelitos. Es así como, (Montes Vozmediano, Pastor Ruiz, Martín Nieto, & Atuesta Reyes, 2020) resalta como a partir de las redes sociales brindan a los delincuentes una plataforma para llevar a cabo estafas y campañas de phishing, y también pueden ser utilizadas para la difusión de malware y la desinformación. Las transformaciones sociales, como la dependencia cada vez mayor de las redes sociales y la digitalización de nuestras vidas cotidianas, han hecho que las personas sean más vulnerables a las amenazas cibernéticas.

La globalización y la ausencia de fronteras en línea plantean desafíos en la persecución de ciberdelincuentes, ya que sus acciones suelen trascender fronteras nacionales, complicando la identificación y el castigo. Según (Aliaga Díaz, 2022), la cooperación internacional es esencial en la lucha contra estos delitos, respaldada por acuerdos y tratados globales. La compleja relación entre ciberdelitos, evolución tecnológica y transformaciones sociales está en constante cambio. La adopción de medidas de ciberseguridad efectivas, educación pública sobre riesgos cibernéticos y la colaboración entre gobiernos, empresas y ciudadanos son cruciales para abordar estas amenazas en evolución y proteger la seguridad en línea en una sociedad cada vez más digitalizada.

CONCLUSIONES

La investigación ofrece una visión integral de la ciberseguridad en Colombia, resaltando la importancia de abordarla desde el Derecho Administrativo en una

sociedad digitalizada. Se identifica un panorama complejo y en constante evolución, destacando la integración parcial de la ciberseguridad en el ordenamiento jurídico colombiano. Asimismo, se observa cómo diversas dependencias estatales, en el contexto del gobierno digital, han implementado sistemas digitales más seguros y accesibles para la comunidad.

Además de resaltar los desafíos en la consolidación del gobierno digital, se señalan las dificultades asociadas a la modernización administrativa mediante tecnología, destacando la necesidad apremiante de abordar proactiva y eficazmente la ciberseguridad, lo que plantea desafíos significativos. Se analiza la necesidad de consolidar políticas públicas digitales desde la perspectiva del buen gobierno, evaluando la efectividad de la administración pública en la prevención de delitos cibernéticos, considerando la evolución tecnológica y sus implicaciones sociales. Esto resalta la importancia de la cooperación internacional y la concienciación pública en la lucha contra las amenazas cibernéticas.

En conclusión, este artículo enfatiza la necesidad de incorporar las nuevas tecnologías en la administración pública, lo cual permitirá abordar los cambios y transformaciones sociales de la era moderna. De igual manera, permite denotar la importancia de llevar a cabo tratados multilaterales a través de los cuales se permita tomar acciones contundentes y conjuntas frente a las problemáticas en materia de ciberseguridad, que se ha convertido en una prioridad crucial en la administración pública, y su abordaje desde una perspectiva legal y gubernamental sólida es esencial para garantizar la seguridad en línea de los ciudadanos y la eficacia de la gestión gubernamental en la era digital.

Referencias

Aguirre, R., & Jiménez , C. (2020). Tecnologías de la información y la comunicación para la conservación y promoción de la diversidad cultural en el marco del pluralismo jurídico. *Revista digital de Derecho Administrativo, 22*, 1- 15.

Alegre Rodríguez, L., & Padilla López, R. (2023). GOBIERNO DIGITAL, MODERNIZACIÓN DEL ESTADO Y SERVICIO AL CIUDADANO Consideraciones en una estrategia de gobierno digital en Perú. *VISUAL Review. International Visual Culture Review , 13*(2), 1-8. doi:https://doi.org/10.37467/revvisual.v10.4567

Aliaga Díaz, C. (2022). El futuro de la cooperación penal internacional para la investigación de ciberdelitos en el segundo protocolo adicional al convenio de cibercriminalidad. *Universidad Siglo 21. Trabajo de grado de Especialización*, 1. 61. Obtenido de https://repositorio.uesiglo21.edu.ar/handle/ues21/26275

Álvarez Goyoaga, G. (2019). Incidencia actual del derecho “blando” en el Derecho Internacional. *Revista Diplomática - 2ª Época, 1*(2), 1- 189. Obtenido de https://www.academia.edu/download/63906169/Rev._Dip._v1_n2_120200713-35097-ora1p7.pdf

Chávez Ramos, A. (2018). Información y participación ciudadana en el contexto del gobierno abierto: las potencialidades de la biblioteca pública. *Biblios*(68), 34- 47. doi:https://doi.org/10.5195/biblios.2017.350

Congreso de la República de Colombia. (2009). *Ley 1273.* Bogotá D.C: Diario Oficial No. 47.223. Obtenido de http://secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso de la República de Colombia. (2009). *Ley 1341.* Bogotá D.C: Diario Oficial No. 47.426. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html

Congreso de la República de Colombia. (2012). *Ley 1581.* Bogotá D.C: Diario Oficial No. 48.587. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Congreso de la República de Colombia. (2014). *Ley 1712.* Bogotá D.C: Diario Oficial No. 49.084. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html

Consejo de Europa. (2021). *Convención de Budapest sobre la ciberdelincuencia.* Estrasburgo: Consejo de Europa. División de Ciberdelito.

Consejo Nacional de Política Económica y Social. (2010). *CONPES 3650.* Bogotá D.C: Departamento Nacional de Planeación.

Consejo Nacional de Política Económica y Social. (2016). *CONPES 3854.* Bogotá D.C: Departamento Nacional de Planeación. Obtenido de https://colaboracion.dnp.gov.co/cdt/conpes/econ%C3%B3micos/3854.pdf

Consejo Nacional de Política económica y social. (2019). *Documento CONPES 3975. Política para la Transformación Digital e Inteligencia Artificial.* Bogotá D.C: Departamento Nacional de Planeación.

Fernández Valenzuela, L., Fernández Ocaña, Y., Hidalgo Soto, C., Aliaga Cotrina, J., & Fuster-Guillén, D. (2023). E-Government and its Development in the Region: Challenges. *International Journal of Professional Business Review, 8*(1), 1- 15. doi:https://doi.org/10.26668/businessreview/2023.v8i1.939

Ferriz Sánchez, R. (2022). Participación ciudadana y Buen Gobierno democrático. Posibilidades y límites en la era digital. *Revista Espanola de Derecho Constitucional*(125), 341- 355.

Figueroa G., R. (2013). El derecho a la privacidad en la jurisdicción de protección. *Revista Chilena de Derecho, 40*(3), 859- 889. doi:10.4067/s0718-34372013000300005

Gurría, J. A. (2009). El buen gobierno para el desarrollo económico y social. Revista del CLAD Reforma y Democracia. *Revista del CLAD Reforma y Democracia*, 7- 22.

Hamdi , K., Padilla, J. J., Vernon-Bido, D., Saikou, Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: state of the art and future directions. *Journal of Cibersecurity*, 1- 13. doi:https://doi.org/10.1093/cybsec/tyab005

Jara Fuentealba, N., & Jorquera Cruz, A. (2021). La responsabilidad de la Administración del Estado por incidentes de ciberseguridad. *Revista Chilena de Derecho y Tecnología, 10*(1), 201- 230. doi:http://dx.doi.org/10.5354/0719-2584.2021.58776

Jiménez-Pitre, I., Martelo, R., & Jaimes, J. (2017). Escuela de gobierno basada en TIC: Determinante para la accesibilidad e integralidad del empoderamiento digital. *Informacion Tecnologica, 28*(5), 75- 86. doi:http://dx.doi.org/10.4067/S0718-07642017000500010

Lafioune, N., Desmarest, A., Poirier, É. A., & St-Jacques, M. (2023). Digital transformation in municipalities for the planning, delivery, use and management of infrastructure assets: Strategic and organizational framework. *Sustainable Futures, 6*, 1- 16. doi:https://doi.org/10.1016/j.sftr.2023.100119

Montes Vozmediano, M., Pastor Ruiz, Y., Martín Nieto, R., & Atuesta Reyes, J. D. (2020). Smartphone y redes sociales: una aproximación a los usos, vulnerabilidades y riesgos durante la adolescencia en España y Colombia. *Revista ESPACIOS, 41*(48), 44- 59. doi:10.48082/espacios-a20v41n48p04

Muñoz Flores, F., Barroso Gutiérrez, J., & García Báez, A. (2022). Estandarización digital, vulnerabilidad social y gobierno abierto: el caso de XBRL en Europa. *Revista Espanola de la Transparencia*(15), 313- 327. doi:https://doi.org/10.51915/ret.222

Oltra Català, L., & Verdú Penalva, C. (2020). El desarrollo del e-gobierno en los pequeños municipios de la comunidad valenciana (España): más espejo que cristal. *Ager*(29), 39- 77. doi:10.4422/ager.2020.02

Pirni, A., Giampellegrini, P., & Raffini, L. (2019). Digital transformation and egovernment. For a research agenda on the Liguria region. *OBETS, 14*(2), 471- 490. doi:10.14198/OBETS2019.14.2.07

Pons Gamón, V. (2017). Internet, la nueva era del delito: ciberdelito,ciberterrorismo,legislación y ciberseguridad. *URVIO Revista Latinoamericana de Estudios de Seguridad*, 80- 93. doi:https://doi.org/10.17141/urvio.20.2017.2563

Presidencia de la República de Colombia. (2022). *Decreto 322.* Bogotá D.C: Diario oficial. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866

Sarmiento Loaiza, R. (2023). Políticas públicas como promotoras de la implementación de las tecnologías de la información y las comunicaciones -TIC- en las instituciones educativas oficiales de Medellín entre el 2016 y 2021. *Universidad Pontificia Bolivariana. Tesis de Maestría*, 1- 66. Obtenido de http://hdl.handle.net/20.500.11912/10582

Solé Ponce, J. (2023). Buen gobierno y derecho a una buena administración desde una perspectiva de calidad normativa. A propósito del libro de la profesora Maria De Benedetto, Corruption from a Regulatory Perspective. *Eunomia. Revista en Cultura de la Legalidad*(24), 377- 401. Obtenido de 10.20318/eunomia.2023.7679

Tavares, A., & Bitencourt, C. (2021). Diálogo entre o Direito e a Engenharia de Software para um novo paradigma de transparência: controle social digital. *Revista Eurolatinoamericana de Derecho Administrativo, 8*(1), 9- 34. doi:https://doi.org/10.14409/redoeda.v8i1.9676

Toscano, M. (2017). Sobre el concepto de privacidad: la relación entre privacidad e intimidad. *Revista Isegoria*(57), 533-552.