Universidad Hispanoamericana

Facultad de Derecho

Tesis para optar por el grado académico de Licenciatura en Derecho

Derecho Administrativo Digital: Propuestas para su implementación basadas en el marco normativo costarricense y el derecho comparado.

Autores

Ignacio Rafael Sanabria Céspedes
113990115

Julissa Valerio Berrocal
402540330

Tutor

Lic. Rodolfo Sotomayor Aguilar

San José, Costa Rica

2025

DECLARACIÓN JURADA

DECLARACIÓN JURADA

Yo Ignacio Sanabria Céspedes, mayor de edad, portador de la cédula de identidad número 1-1399-0115 egresado de la carrera de Derecho de la Universidad Hispanoamericana, hago constar por medio de éste acto y debidamente apercibido y entendido de las penas y consecuencias con las que se castiga en el Código Penal el delito de perjurio, ante quienes se constituyen en el Tribunal Examinador de mi trabajo de tesis para optar por el título de licenciatura, juro solemnemente que mi trabajo de investigación titulado: Derecho Administrativo Digital: Propuestas para su implementación basadas en el marco normativo y el derecho comparado., es una obra original que ha respetado todo lo preceptuado por las Leyes Penales, así como la Ley de Derecho de Autor y Derecho Conexos número 6683 del 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 del 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte; articulo 70. Es permitido citar a un autor, transcribiendo los pasajes pertinentes siempre que éstos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor de la obra original. Asimismo, quedo advertido que la Universidad se reserva el derecho de protocolizar este documento ante Notario Público.

En fe de lo anterior, firmo en la ciudad de San José, a los 8 días del mes de febrero del año dos mil veintiseis.

Firma del estudiante

Cédula: 1-1399-0115

DECLARACIÓN JURADA

Yo Julissa Valerio Berrocal, mayor de edad, portador de la cédula de identidad número 4-0254-0330 egresado de la carrera de Derecho de la Universidad Hispanoamericana, hago constar por medio de éste acto y debidamente apercibido y entendido de las penas y consecuencias con las que se castiga en el Código Penal el delito de perjurio, ante quienes se constituyen en el Tribunal Examinador de mi trabajo de tesis para optar por el título de Licenciatura en Derecho, juro solemnemente que mi trabajo de investigación titulado: Derecho Administrativo Digital: Propuestas para su implementación basados en el marco normativo costarricense y el derecho comparado, es una obra original que ha respetado todo lo preceptuado por las Leyes Penales, así como la Ley de Derecho de Autor y Derecho Conexos número 6683 del 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 del 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte; articulo 70. Es permitido citar a un autor, transcribiendo los pasajes pertinentes siempre que éstos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor de la obra original. Asimismo, quedo advertido que la Universidad se reserva el derecho de protocolizar este documento ante Notario Público.

En fe de lo anterior, firmo en la ciudad de San José, a los 08 días del mes de Febrero del año dos mil veintiseis.

Julissa Valerio

Firma del estudiante

Cédula: 402540330

CARTA DEL TUTOR

CARTA DEL TUTOR

Puntarenas, 2 de diciembre del 2025

Lic. Piero Vignoli Chessler
Facultad de Derecho
Universidad Hispanoamericana

Estimado señor:

Los estudiantes Ignacio Rafael Sanabria Céspedes, cédula de identidad número: 113990115 y Julissa Valerio Berrocal, cédula de identidad número: 402540330, me han presentado, para efectos de revisión y aprobación, el trabajo de investigación denominado "***Derecho Administrativo Digital: Propuestas para su implementación basadas en el marco normativo costarricense y el derecho comparado***", el cual han elaborado para optar por el grado académico de Licenciatura en Derecho.

En mi calidad de tutor, he verificado que se han hecho las correcciones indicadas durante el proceso de tutoría y he evaluado los aspectos relativos a la elaboración del problema, objetivos, justificación; antecedentes, marco teórico, marco metodológico, tabulación, análisis de datos; conclusiones y recomendaciones.
Asimismo, indico que el presente trabajo final de graduación fue sometido al análisis de la Plataforma TURNITIN de control anti plagio, siendo satisfactorio su resultado según las normas universitarias

De los resultados obtenidos por los postulantes, se obtiene la siguiente calificación:

a)	ORIGINAL DEL TEMA	10%	10
b)	CUMPLIMIENTO DE ENTREGA DE AVANCES	20%	20
C)	COHERENCIA ENTRE LOS OBJETIVOS, LOS INSTRUMENTOS APLICADOS Y LOS RESULTADOS DE LA INVESTIGACION	30%	30
d)	RELEVANCIA DE LAS CONCLUSIONES Y RECOMENDACIONES	20%	20
e)	CALIDAD, DETALLE DEL MARCO TEORICO	20%	20
	TOTAL		100

En virtud de la calificación obtenida, se avala el traslado al proceso de lectura.

Atentamente,

RODOLFO SOTOMAYOR AGUILAR (FIRMA)
Digitally signed by RODOLFO SOTOMAYOR AGUILAR (FIRMA)
Date: 2026.02.05 11:15:28 -06'00'

Lic. Rodolfo Sotomayor Aguilar
Cédula identidad 602690071
Carné Colegio Profesional 9762

CARTA DEL LECTOR

UNIVERSIDAD HISPANOAMERICANA
Seriedad y Prestigio

CARTA DEL LECTOR

Heredia, 1 de febrero de 2026

Prof. Piero Vignoli Chesler
Director de la Carrera de Derecho
Universidad Hispanoamericana

Estimado señor:

Los estudiantes Ignacio Rafael Sanabria Céspedes, cédula de identidad 1-1399-0115 y Julissa Valerio Berrocal, cédula de identidad 4-0254-0330 me ha presentado, para efectos de revisión y aprobación, el trabajo de investigación denominado "*Derecho Administrativo Digital: Propuestas para su implementación basadas en el marco normativo costarricense y el derecho comparado*", el cual ha elaborado para optar por el grado de Licenciados en Derecho.

He revisado el trabajo asignado en segunda revisión de fecha 22 de enero de los corrientes y he determinado que el mismo **CUMPLE** con los requisitos mínimos para avalar la investigación. Por consiguiente, este trabajo cuenta con mi aval para ser presentado en la defensa pública respectiva.

Atentamente,

CARLOS JOSE MEJIAS RODRIGUEZ (FIRMA)
Firmado digitalmente por CARLOS JOSE MEJIAS RODRIGUEZ (FIRMA)
Fecha: 2026.02.01 21:49:41 -06'00'

Prof. Mag. Carlos José Mejías Rodríguez

Universidad Hispanoamericana

Lector

Ced. 1-1231-0312

Carné del Col de Abo. 19536

DECLARACIÓN JURADA DEL CENIT

UNIVERSIDAD HISPANOAMERICANA
CENTRO DE INFORMACION TECNOLOGICO (CENIT)
CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCION PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DE LOS TRABAJOS FINALES DE GRADUACION

San José, 8 de febrero de 2026

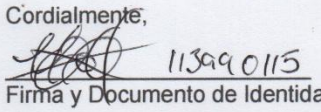
Señores:
Universidad Hispanoamericana
Centro de Información Tecnológico (CENIT)

Estimados Señores:

El suscrito (a) Ignacio Sanabria Céspedes con número de identificación 1-1399-0113 autor (a) del trabajo de graduación titulado Derecho Administrativo Digital: Propuestas para su implementación basadas en el marco normativo costarricense y el derecho comparado.
presentado y aprobado en el año 2026 como requisito para optar por el título de Licenciatura en Derecho; (X / NO) autorizo al Centro de Información Tecnológico (CENIT) para que con fines académicos, muestre a la comunidad universitaria la producción intelectual contenida en este documento.

De conformidad con lo establecido en la Ley sobre Derechos de Autor y Derechos Conexos N° 6683, Asamblea Legislativa de la República de Costa Rica.

Cordialmente,



113990113
Firma y Documento de Identidad

UNIVERSIDAD HISPANOAMERICANA
CENTRO DE INFORMACION TECNOLOGICO (CENIT)
CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCION PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DE LOS TRABAJOS FINALES DE GRADUACION

San José, 08 de Febrero, 2026

Señores:
Universidad Hispanoamericana
Centro de Información Tecnológico (CENIT)

Estimados Señores:

El suscrito (a) Julissa Valeria Berrocal con número de identificación 402540330 autor (a) del trabajo de graduación titulado Derecho Administrativo Digital: Propuestas para su implementación basados en el marco normativo costarricense y el derecho comparado
presentado y aprobado en el año 2026 como requisito para optar por el título de Licenciatura de Derecho; (SI / NO) autorizo al Centro de Información Tecnológico (CENIT) para que con fines académicos, muestre a la comunidad universitaria la producción intelectual contenida en este documento.

De conformidad con lo establecido en la Ley sobre Derechos de Autor y Derechos Conexos N° 6683, Asamblea Legislativa de la República de Costa Rica.

Cordialmente,

Julissa Valeria 402540330
Firma y Documento de Identidad

DEDICATORIA

Julissa

A mis padres, que sin ellos esto jamás hubiera sido posible.

Ignacio

A mi madre por nunca dejar de creer en mí y apoyarme en todas mis locuras; y a mi hijo Nicolas, si él supiera el orgullo de ser su padre y lo que me motiva a ser mejor persona y profesional.

AGRADECIMIENTOS

Julissa

A Dios, en primer lugar, por permitirme llegar hasta aquí y por brindarme la fuerza y el entendimiento para seguir adelante aun en los momentos más difíciles.

A mis padres, Mario y Maribel, que, con esfuerzo, sacrificio y un amor inmenso me dieron la oportunidad de estudiar esta carrera y abrirme camino en esta vida. Gracias por creer en mí incluso cuando yo misma no dimensioné todo lo que hicieron para que pudiera llegar hasta aquí y me enseñaron que para cumplir mis sueños debo luchar incansablemente por ellos.

A mis familiares y seres queridos: Mis hermanos mayores José Mario, Daniela y Marco por soportarme y ser mi apoyo incondicional. Jessiel, mi sobrina, quien quiero ser un ejemplo para su vida. No Rae, mi gran compañera de estudio, que estuvo a mi lado durante todo este proceso académico, compartiendo largas noches, lágrimas y cada pequeño triunfo. A mi abuela Emilce, por haber vivido lo suficiente para verme convertirme en profesional, a pesar de los años y la enfermedad, y por llamarme siempre su *flor del jardín*. Este logro también te pertenece.

A los profesores de la carrera de Derecho que me han formado desde lo académico y profesional. A mis compañeros, amigos y futuros colegas, quienes formé una estrecha relación durante este camino de estudio. En especial a Ignacio, mi compañero de tesis y mejor amigo, con quien tuve el honor de compartir este gran viaje de la carrera universitaria desde sus inicios y a quien espero seguir viendo crecer profesionalmente.

Ignacio

Quiero agradecer primeramente a la vida, porque me hizo entender que a veces hasta cuando escribe torcido, siempre escribe perfecto. Seguidamente a mi familia, especialmente a mi mamá Miriam, mi papá Rafael (q.d.D.g), mi abuela Irene (q.d.D.g), mi hermana Ingrid, mis sobrinos Daniel y Alejandro, y en mayor medida a mi hijo Nicolas que desde que llegó a mi vida me convirtió en mejor persona; a todos ellos les agradezco las risas, las tristezas, los enojos y los momentos vividos.

A Silvia Herrán (q.d.D.g.) y Jennifer Díaz, sin ellas no sabría que sería de mí, su guía, regaños y enseñanzas demostraron que árbol que nace torcido, sí puede ser enderezado.

A todos mis compañeros de la Universidad Hispanoamericana con los que alguna vez compartí, especialmente a los que en algún momento me abrieron la puerta de sus hogares y de sus familias, como Guido, Fonseca, Emily y Krystel, pero en especial mi grupo de Extraditables: Fiorella, Franciny, Jazmín, Kendall, Sarely y Yitza. Y más especialmente a Julissa, mi compañera de tesis, que no solo compartió el proceso de este trabajo investigativo si no que ha sido mi amiga desde nuestro primer cuatrimestre en el lejano 2021, la seguiré molestando hasta el fin de los tiempos.

A mis compañeros y profesores que me acompañaron en el Comité Estudiantil, Melissa, Natalia, Pablo, Adriana, Armando, María Fernanda, Joice, Danny y los profesores Christian, Piero, Marco y Juan Carlos de todos he aprendido un montón. Adicionalmente a todos los profesores con los que estuve durante estos 4 años, en especial al Lic. Rodolfo Sotomayor por aceptar ser nuestro tutor de tesis.

A mi novia Sharon, que me ha soportado en este sprint final para lograr este objetivo, te amo y gracias por ser parte de mi vida.

Y finalmente pero no menos importante, quiero agradecerme a mí mismo, que he aprendido a ser resiliente a través de los años, y cuando la pandemia afectó el mundo, decidí tomar esa crisis y convertirla en oportunidad, y aquí estoy, a pesar de sobrevivir momentos muy oscuros en mi vida, me siento un ganador. Me prometo seguir creciendo.

TABLA DE CONTENIDOS

RESUMEN

La investigación desarrolla un análisis normativo sobre la digitalización en los procedimientos de gestión administrativa en Costa Rica, en el marco de los principios generales de la administración pública, la protección de datos y la accesibilidad. Los objetivos tanto general como específicos buscan examinar cómo la normativa vigente ha sido implementada en la Administración Pública, identificando desafíos y oportunidades, y proponiendo recomendaciones fundamentadas en la doctrina y el derecho comparado.

Metodológicamente, el estudio se sustenta en un enfoque cualitativo de carácter interpretativo y explicativo, apoyado en normativa nacional e internacional, doctrina especializada, entrevistas y análisis comparado con las experiencias de Estonia y Chile.

Los principales hallazgos evidencian una serie de vacíos, conflictos y tensiones regulatorias que obstaculizan la consolidación del Derecho Administrativo Digital en Costa Rica. Se destaca la ausencia de un marco legal central y coherente, la fragmentación normativa y la prevalencia de reglamentos y decretos ejecutivos sin fuerza vinculante; conflictos de gobernanza y competencias entre instituciones; tensiones en la aplicación de principios jurídicos clásicos como legalidad y proporcionalidad en entornos digitales; vacíos normativos en materia de protección de datos biométricos, interoperabilidad y certificación digital; así como rigidez en los mecanismos de autenticación digital y obstáculos para la interoperabilidad administrativa. Asimismo, se identifican desafíos estructurales vinculados a la falta de voluntad política, la brecha territorial en el acceso a internet y el riesgo de exclusión social en la transición hacia lo digital.

La conclusión central sostiene que la digitalización del Derecho Administrativo en Costa Rica es un proceso urgente e irreversible, pero requiere una transformación normativa y organizacional profunda. Se propone la creación de un órgano desconcentrado adscrito al MICITT

que unifique competencias dispersas, fortalezca la interoperabilidad interinstitucional y consolide un marco jurídico sólido que garantice seguridad, eficiencia y respeto a los derechos fundamentales.

Palabras clave: Derecho Administrativo Digital, gobierno digital, protección de datos, interoperabilidad.

Capítulo I - INTRODUCCIÓN

1.1.Planteamiento del Problema

La evolución tecnológica a través de los años ha permitido que la digitalización no sea únicamente una herramienta viable, sino que se ha convertido en una necesidad para el desarrollo social. El proceso continuo ha impulsado, desde antes de 2020, avances que han permitido la evolución de estructuras de producción, tramitación, educación e interacción social. No obstante, fue hasta la Pandemia de COVID-19, debido a las restricciones sanitarias y el confinamiento, que la población mundial se vio obligada al uso de herramientas digitales de forma masiva para satisfacer las demandas laborales, académicas y las relaciones interpersonales desde el hogar.

Ante esta situación, la Administración Pública no ha sido ajena a dicha evolución digital. Esto debido a su rol en responder ante las necesidades demandadas de los administrados, donde se ha exigido un servicio más eficiente, accesible, facilitador y transparente en el sector público conforme se ha ido dando dicha transformación. No obstante, la promulgación de la digitalización se ha visto dispersada, ya que cada institución estatal ha buscado la manera de implementar desde su propia capacidad y presupuesto, generando una multiplicidad y disparidad de interfaces heterogéneas que brindan dificultades sobre el control interno institucional. Dicha fragmentación

impacta negativamente al administrado, quien, en el ejercicio de sus gestiones, se ve compelido a suministrar su información personal de forma reiterada ante diversas instancias estatales.

Con el fin de afianzar la digitalización, este objetivo debe ser conforme al Principio de Legalidad, estipulado en el artículo 11 de la Constitución Política de la República de Costa Rica y el mismo numeral de la Ley General de la Administración Pública, que expresa lo siguiente:

> 1. La Administración Pública actuará sometida al ordenamiento jurídico y sólo podrá realizar aquellos actos o prestar aquellos servicios públicos que autorice dicho ordenamiento, según la escala jerárquica de sus fuentes.
>
> 2. Se considerará autorizado el acto regulado expresamente por norma escrita, al menos en cuanto a motivo o contenido, aunque sea en forma imprecisa.

Este principio base del Derecho Administrativo, se interpreta de manera que todo acto administrativo debe estar previamente fundamentado en la normativa jurídica que promulgue el Estado. Sin perjuicio de lo anterior, este principio se concatena con el principio de Reserva de Ley, mismo que es aplicable únicamente en el caso de las potestades de imperio conforme al artículo 12 inciso 2 de la Ley General de Administración Pública. Dicho principio, anteriormente mencionado, le brinda la potestad al Poder Legislativo para ser el promulgador de la ley formal según el artículo 121 de la Constitución política y el artículo 59 inciso 1 de la Ley General de Administración Pública.

Sin embargo, la problemática se podría deducir que se debe a que los intentos de promover un marco normativo que regule y fomente la digitalización dentro del Derecho Administrativo han sido temporalmente dispersos y desvinculados, esto debido a que los esfuerzos que se han realizado mediante política públicas, decretos ejecutivos y algunas leyes no han sido los esperados por la ciudadanía y el sistema. Un hecho provocador, es que los principios que rigen y le otorgan rigidez

a la función administrativa, no se plasman de manera real, obligando a que se aplique la discrecionalidad administrativa al momento de digitalizar los servicios, por un marco legal que no lo sustenta firmemente.

A partir de esto, se empieza a observar que la digitalización se ha ido involucrando de manera "natural" en la sociedad y en consecuencia en las distintas ramas del derecho, puede que no esté integrando de forma armónicamente al Derecho Administrativo.

1.2.Antecedentes

1.2.1 Evolución del Derecho administrativo y el reto de la era digital.

Desde una perspectiva inicial, para entender la coyuntura actual en la que se encuentra el Derecho Administrativo, se debe analizar el desarrollo de este a través de la historia. Esto debido a que se ha experimentado varias transformaciones que han sido impulsadas por eventos políticos, sociales y tecnológicos. Todos estos hechos fueron los causantes de la redefinición en la relación del Estado con los ciudadanos.

A fin de encausar este devenir histórico, se debe mencionar la Revolución Francesa y los ideales de la Ilustración, que trajeron consigo el cambio coyuntural con el derrocamiento de la monarquía como forma de gobierno, y siendo este sustituido por el concepto de Estado-Nación. No obstante, cabe aclarar que las ideas que originaron este cambio en la forma organizativa del poder que conlleva al nacimiento de la Administración Pública, y genera el asentamiento de las bases jurídicas de las funciones administrativas del Estado, no nacen durante este período histórico.

De manera que los pensadores revolucionarios desde un juicio reflexivo de conceptos como el de las polis griegas o las civitas romanas dan forma a los conceptos de Estado, administración y justicia, determinando bases que conllevan a la separación de poderes y el sistema de control

entre ellos mismos, como menciona Spacarotel (2020, p. 6), esto llego a significar la creación de "reglas de gobierno y el respeto a los derechos de las personas, eran de obligatorio cumplimiento tanto para gobernados como gobernantes".

Paralelamente el desarrollo de la Revolución Industrial, "desde el neolítico (...) la humanidad no había experimentado una serie de transformaciones tan importantes en cuanto a su economía, su productividad, aparición de nuevas tecnologías, qué conllevo a una transformación profunda de la sociedad" (Academia Play, 2019, 0m16s), con el desarrollo de este acontecimiento, se impuso nuevas demandas sociales sobre las mesas de las administraciones, y empuja a un proceso de cimentación jurídica capaz de gestionar las sociedades industriales.

En consecuencia, "se produce el proceso de construcción jurídico-político de los Estados Nación que, a su vez, da lugar al nacimiento del sujeto que es objeto de las políticas (...), la Administración pública como subsistema que adopta la burocracia" (Cortés Abad, 2020, p. 8). Erigiendo a su vez las bases de un Estado interventor y regulador, desligándose del rol de espectador debido a la insostenibilidad que suponía la migración masiva a grandes ciudades, condiciones laborales, salud pública y urbanismo descontrolado, propiciando normativas especificas en estos ámbitos, y adicionalmente se crea el concepto de Servicio Público debido a la necesidad de que el Estado regule a través de entidades administrativas su prestación.

Terminando este hito histórico se debe hacer mención del fallo Arrêt Blanche del Tribunal de Conflictos francés en 1873, que inicia un proceso de separación entre lo que son las decisiones administrativas y las judiciales, propiciando la creación de cuerpos normativos y principios propios del Derecho Administrativo, así como lo menciona Spacarotel (2020, p.10):

> El Consejo de Estado fue entonces creando precedentes jurisprudenciales y surgiendo así los principios modernos del Derecho Administrativo que influenciaron a gran número de

países. Algunos de estos son: principio de legalidad, de presunción de legalidad, la diferenciación de contratos administrativos y contratos entre particulares, el de culpa o falla del servicio para sustentar responsabilidad de la administración, principios de la función pública, la diferenciación entre bienes del Estado y bienes de particulares.

Continuando con el tercer hito de transformación, el cual se da a mediados del siglo XIX, posterior a la Segunda Guerra Mundial. En ese momento se asienta el concepto del Estado del Bienestar, que empapa a la Administración Pública de un contrato social que adopta políticas que presentan al Estado como un protagonista más amplio en la intervención socioeconómica de los Estados, y por ende el Derecho Administrativo se vuelve más complejo y técnico, y consigo, muchos países deciden constitucionalizar los principios del Derecho Administrativo.

Durante este periodo Costa Rica deja atrás lo sencillo y rudimentario de su sistema administrativo, el cual tenía normas dispersas, pocos organismos gubernamentales especializados y sin ningún ente en la materia contencioso administrativo que amparara al administrado en caso de una arbitrariedad de la Administración.

La promulgación de la Constitución Política de 1949 es un parteaguas que establece las bases para que Costa Rica se convierta en un Estado de Derecho, que como hito no solo sentó las bases del Derecho Administrativo actual costarricense, sino que además trae consigo varias reformas sociales y económicas que siguen siendo de gran importancia para el país; la abolición del ejército, el Código de Trabajo, la Caja Costarricense del Seguro Social, las garantías sociales, entre otras. A partir de este momento se puede hacer mención del Derecho Administrativo Costarricense, aunque como cualquier proceso de implementación y desarrollo fue necesario varios años para curtir la normativa.

Posteriormente entre las décadas de 1970 y 1980, el Derecho Administrativo sufre otra transformación de la mano de las crisis económicas mundiales. Esto se debió al repercutir fuertemente en las economías, se empezaron hacer cambios que llegaron "para orientar a la Administración pública hacia principios de eficacia, eficiencia o economía de recursos.*"* (Cortés Abad, 2020, p. 9). Resultando en el proyecto de la Ley General de Administración Pública promulgada en 1978 con la voluntad de dotar de orden y eficiencia a la administración, esta ley encontró sus bases en tendencias doctrinales europeas, donde se discutían en el seno de la Administración desde la década de los años 60. Es con ayuda del jurista costarricense Eduardo Ortiz Ortiz, logra ver la luz para dotar al Derecho Público costarricense de un carácter sistemático, principios bien definidos, discrecionalidad administrativa limitada y mayor seguridad jurídica.

Desde ese momento hasta el día de hoy en pleno siglo XXI, el Derecho Administrativo y la Administración Pública han ido sufriendo cambios y reformas ya sea en sus leyes, decretos o reglamentos, subyacentemente ha sido la sociedad y la tecnología, esta última que ha evolucionado de manera drástica.

Actualmente el Derecho Administrativo se encuentra en un momento histórico que ha sido llamado Revolución Industrial 4.0., mismo que esta coyuntura trascendental presenta la necesidad urgente de digitalización. En este punto de inflexión no solo representa la incorporación de herramientas tecnológicas en las gestiones administrativas, sino más bien se está ante un panorama de replanteamiento normativo, ético y operativo del vínculo de la administración y el ciudadano en los entornos digitales.

Se debe concluir qué con la comprensión de los hitos históricos que han reformado esta rama del derecho, sumado a las necesidades que cada día presionan un cambio actualmente, hace

prever que la humanidad se encuentra en una etapa trascendental, por lo que se debe proyectar los desafíos y las oportunidades de la actualidad que se moldeen el futuro.

1.2.2. ¿Por qué Derecho Administrativo Digital?

Se emplea el término de *Derecho Administrativo Digital* como expresión para abordar la temática de esta investigación, ya que obedece a la necesidad de adoptar un concepto más amplio y transversal que permita un abordaje integral de la actual transformación del Derecho Administrativo en la era de las tecnologías de la información y comunicación.

Dicho de otra manera, durante las últimas décadas los juristas han visto la transformación que han sufrido los presupuestos sociales, económicos, políticos y hasta culturales a través de la revolución tecnológica. El ciberespacio actualmente no solo es un entorno de interacción humana, si no que se ha convertido en un espacio de intercambios de mercancía, adquisición de bienes y servicios, mercado de nuevas riquezas, fuentes de trabajo y más.

Ante esta situación, surge en primer orden el derecho informático, y Barrio (2024, p.38) citando a Pérez Luño (1996), lo define "como la rama de los ordenamientos jurídicos contemporáneos integrada por el conjunto de disposiciones dirigido a la regulación de las nuevas tecnologías de la información y la comunicación, es decir, la informática y la telemática". El autor trae a colación varios temas de discusión además de la definición anteriormente mencionada, ya que por sí misma, hace referencia a una rama interdisciplinar que puede abarcar desde el derecho hasta la informática jurídica, la cual esta última la define como "la relativa al tratamiento automatizado de las fuentes de conocimiento jurídico —legislación, jurisprudencia y doctrina" (Barrio, 2024, p.39).

Sumado a que el Derecho Informático se empieza a desarrollar en tres etapas; la primera que inicia en la década del 60, y la última cierra con la llegada del internet y la creación de algunas

materias especializadas en Estados Unidos. Estas tres etapas se consolidan con la finalidad de frente a los problemas que se estaban generando en cada una de ellas: como lo fue el Derecho de Internet, Derecho del Ciberespacio o el Ciber derecho, culminando en Derecho basado en Tecnologías de la Información y la Comunicación. Sin embargo, como el autor menciona parafraseando a García Mexía "resulta inadecuada pues prescinde de Internet como término-fuerza, cuando Internet ha sido el verdadero revulsivo de la revolución digital" (Barrio, 2024, p. 40).

En contraste, el derecho digital ha surgido en los últimos años como definición los problemas que surgen en la actualidad jurídicamente, esto respondiendo a tres situaciones básicas, y que Barrio (2024, p.42) enumera de la siguiente manera:

> En primer lugar, la necesidad de contar con una respuesta jurídica precisa para toda la actividad relacionada con los servicios de la sociedad de la información -y ahora sociedad digital- que disponga su propia regulación, lenguaje y elementos axiológicos. En segundo lugar, del efecto transversal que las tecnologías, sobre todo Internet y ahora las tecnologías disruptivas, están suponiendo en nuestras vidas y por ende en el resto de las tradicionales ramas del Derecho. Y, tercer lugar, de promulgar algunas normas jurídicas nuevas para dar respuesta a los cambios que introduce la Cuarta Revolución Industrial.

Para el autor anteriormente mencionado, se debe tomar en cuenta lo aspectos como: la información digital, ya que con la entrada del *cloud computing* y el *big data,* en combinación con técnicas de procesamiento de datos a través de Inteligencia Artificial han logrado un volumen y velocidad de procesamiento para análisis que desdibujan lo que tradicionalmente se conocía sobre intimidad y protección de datos. La comunicación se ha transformado desde los medios privados hasta los medios masivos, que abarcan problemáticas que van desde el *spam,* noticias falsas hasta

temas de identidad digital, libertad de expresión, protección de datos o ciberdelincuencia. La convergencia, tema relacionado con la integración en diferentes ámbitos, ya es un tema discutido a nivel europeo relacionado con el principio de campo de juego nivelado dando igualdad de oportunidades a todos los actores del sector digital. Universalidad, este tema yace en la polivalencia de la tecnología, que puede ir desde una Inteligencia Artificial de un vehículo hasta un microchip en una prenda de vestir para seguir el movimiento.

La neutralidad, en contra peso a la apertura de la tecnología hacia el mundo, esta busca una regulación que permita la innovación siempre y cuando respete derechos y libertades. Finalmente, la gestión de riesgos; es una herramienta basada en el riesgo de cumplimiento que busca promover una mayor responsabilidad por parte de los sujetos públicos y/o privados, donde "los deberes y obligaciones de los sujetos obligados se escalonan y adaptan a los riesgos concretos derivados de su actividad especifica" (Barrio, 2024, p.45) por lo que el autor considera que "supera la lógica binaria de cumplimiento/incumplimiento en términos clásicos kelsenianos" (Barrio, 2024, p.45) actualmente conocida como *compliance,* donde se establece una normativa de organización y gestión que integre medidas de control y vigilancia para prevención de incumplimientos normativos con la ventaja que es flexible ya que solo se deben tomar medidas ante la existencia de un riesgo.

En síntesis, sobre la misma evolución que ha sostenido la tecnología, en ámbitos mayormente europeos se ha determinado que la rama del derecho que hoy en día se encarga de estudiar los ámbitos que se dan por las tecnologías basadas en Internet es el Derecho Digital y que para objeto del presente trabajo de investigación será el utilizado para definir el campo de estudio. Cabe destacar, que también existen trabajos académicos que prefieren el uso de otros términos

como el Derecho de Internet o Ciber Derecho, además concuerdan que a futuro se debe hacer una limitación entre estos y el Derecho de los Robots y el Derecho de la Inteligencia Artificial.

1.2.3. Derecho Administrativo frente a la digitalización.

En análisis a la irrupción digital en el Derecho Administrativo, no solo debe ser vista desde la evolución profunda de la forma en que se organiza, gestiona y controla la Administración Pública, ya que no solo los procedimientos administrativos se han visto y se verán impactados en esta frecuente mutabilidad en que las tecnologías de la comunicación e información avanzan. Los institutos, características, nociones y principios que rigen el derecho administrativo y su concepción deberán ser replanteados desde una reflexión teórica que permitan su aplicación a las gestiones administrativas digitales del derecho público.

Primeramente, el derecho administrativo al modernizarse por exigencia de los avances tecnológicos obtendrá, señalado por Piñar Mañas (2011, p.147) en una auto paráfrasis "nuevas herramientas de poder y control, muchísimo más poderosas de las hasta ahora conocidas, y que pueden ser utilizadas sin manifestaciones externas aparentes, pero con resultados inimaginables". Este autor afirmaba en un periodo donde apenas era palpable lo que hoy en día es una realidad, sin embargo, desde ese momento se comenzaba a tener conocimiento sobre el nacimiento de una nueva revolución tecnológica. Desde un enfoque jurídico, se refiere a dilemas que ameritan ser resueltos, y en observancia a lo mencionado por Piñar Mañas (2011) hace una clara referencia al principio de legalidad, con relación a cómo, la administración a través de estas nuevas herramientas que le confieren "poder y control", lo cual se puede utilizar sin que exista una exteriorización evidente del acto.

A modo de ejemplo se pueden citar el caso UPAD del año 2020 que, en síntesis, el Poder Ejecutivo crea la Unidad Presidencial de Análisis de Datos con un tiempo de funcionamiento de

18 meses. Durante este tiempo la Unidad solicitó que varias instituciones y entidades públicas le remitieran información de sus bases de datos, algunas incluían datos sensibles que permitían individualizar esta información. Además de la falta al derecho de autodeterminación informativa, la Unidad vulneró los datos mediante una brecha de seguridad al utilizar una herramienta digital externa de un sitio web llamada Tableau Public, con base en Estados Unidos; esta herramienta de análisis de datos como muchas otras es de pago, pero la UPAD analizó los datos en su versión gratuita la cual no proporciona garantías de seguridad en la información. Dicho acontecer mencionado anteriormente, ilustra cómo el uso actual de información mezclado con un mal uso de herramientas digitales puede provocar que información sensible de ciudadanos costarricense circule por la web.

Con el objetivo de que la Administración Pública evite este tipo de arbitrariedades administrativas en sus actuaciones y debido a la característica de ubicuidad que posee esta rama es que existe una urgencia en desarrollar el tema de modernización y digitalización. Las peculiaridades que hacen al Derecho Administrativo una rama compleja y con diversas áreas de trabajo con peculiaridades bastante heterogéneas, como lo son, la función administrativa, la organización administrativa, responsabilidad administrativa, contratación administrativa, dominio público, empleo público, procedimientos administrativos, proceso contencioso, entre otros. Por lo cual se debe entender que el Derecho Administrativo y sus leyes, reglamentos y decretos son de una disciplina autónoma que no roza el Derecho Privado a menos que por razones de laguna *in extremis* sea necesaria.

Al conjugarse la vertiente del Derecho Administrativo y la necesidad de digitalización, razonando las mismas con el artículo 4 de la Ley General de la Administración Pública que dice:

> La actividad de los entes públicos deberá estar sujeta en su conjunto a los principios fundamentales del servicio público, para asegurar su continuidad, su eficiencia, su adaptación a todo cambio en el régimen legal o en la necesidad social que satisfacen y la igualdad en el trato de los destinatarios, usuarios o beneficiarios.

Este artículo al desgranarse y en apego a lo mencionado anteriormente, se tiene comprender que la Administración Pública tiene el deber de adaptarse a los cambios sociales, económicos y tecnológicos con una finalidad de mantener los principios de eficiencia y continuidad del servicio público.

Por esta razón, se presentan varias interrogantes importantes: ¿Será posible adaptar los diferentes institutos del Derecho Administrativo al entorno digital? ¿Es posible mantener los institutos inalterables o se requiere reinterpretarlos para su uso digital? ¿Las garantías y límites pensados para atar al poder de *imperium* podrán garantizar el actuar administrativo ante los fenómenos digitales?

Con el objeto de responder estas interrogantes es necesario realizar un análisis reflexivo teórico de las bases del Derecho Administrativo en son de comprender si es posible que estos se sigan imponiendo en la era digital manteniendo a el "equilibrio dinámico entre libertad y autoridad, entre derechos del administrado y las potestades públicas ejercidas por la Administración Pública." (Jinesta Lobo, 2001, p.143)

1.3. Problematización

Desde el lanzamiento del iPhone 2G en 2007 acompañado de un auge vertiginoso y sostenido de los teléfonos inteligentes desde el 2010 hasta el día de hoy, el mundo como se conocía ha cambiado. La forma en como las personas, organismos, e incluso la Administración Pública se

relacionan y comunican se ha transformado drásticamente. Las redes sociales, el streaming, el e-commerce, entre muchos otros han plantado una nueva forma de vida.

Pero, a raíz de esta digitalización en la sociedad se puede señalar que el Derecho en general se ha visto rebasado, y el Derecho Administrativo no es la excepción. A pesar de que anterior a este "boom" tecnológico ya la Administración Pública adoptaba ciertos servicios digitales y leyes que apuntaban hacia este horizonte en varios sectores como el municipal, bancario, compras públicas, registral, catastral, entre otros.

Tomando como punto de partida el año 2010 para la presente investigación, y hoy en día se debe determinar que tanto avance dentro del marco del ordenamiento jurídico costarricense existe, siendo la ley de "Creación de la agencia nacional de Gobierno Digital" como el último gran esfuerzo normativo para lograr este objetivo y que enfocada propiamente en la homogenización de las herramientas digitales y cómo estas deben ser aplicadas. Empero, la ley es promulgada en 2021 y se reglamentó hasta 2024 ante orden de la Sala Constitucional conforme el voto 24-18839, la información más actualizada sobre el actuar de la agencia, proviene del noticiero digital "AmeliaRueda.com" del 26 de enero de 2025 donde indica que:

> Se encuentra operando tras la conformación de su Junta Directiva, la cual entre sus decisiones más relevantes destacan la solicitud de insumos al Ministerio de Salud y el Tribunal Supremo de Elecciones sobre las estrategias en cuanto al avance y "visión integral" en materia de Gobierno digital (Siles, A, 2025).

Sumado a lo anterior, en la actualidad las leyes y decretos vigentes de mayor peso normativo, forman parte de un marco normativo desvinculado y provocando la aplicación de la discreción administrativa conforme al artículo 15 de la Ley General de Administración Pública. Por ejemplo, a mencionar se encuentra la "Ley de Protección de la Persona frente al Tratamiento

de sus Datos Personales" N° 8968, vigente desde 2011, que es la cual dispone de una orientación al manejo de la información almacenada en bases de datos. El artículo 1 de esta ley establece "el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad" pero no contempla la capacidad actual de la *big data* que se relacionar a la protección de información y su tratamiento.

En relación, a lo anterior, el ordenamiento jurídico, a través de la Agencia Nacional de Gobierno Digital está buscando consolidar un enfoque en el uso de software y la actualización del hardware, así como la regulación de menor jerarquía como reglamentos, directrices y circulares institucionales. Asimismo, este abordaje puede generar un beneficio en subsanar perdidas de sistemas, problemáticas en el almacenamiento y desecho de equipo tecnológico obsoleto, lo que involucra afectaciones en áreas como la licitación.

Una de las principales dificultades que enfrenta la Administración Pública, y se logran destacar, es el uso de plataformas o servicios propios de sujetos de Derecho Privado donde se licita su uso y ofrecen el servicio a los administrados por el tiempo del contrato. Ante estos mecanismos, pueden llegar a ser efectivos por un plazo de tiempo, sin embargo, pueden ocurrir situaciones que dejan sin la prestación del servicio. Un ejemplo de ello es lo ocurrido entre la empresa española SETEX, y la Municipalidad de San José para el desarrollo la aplicación "Epark CR" en 2024, debido a que cuando se culminó el contrato entre la empresa privada y la institución pública capitalina hubo un desfase que dejó sin servicio de parquímetros por un lapso alrededor de 9 meses, hasta solucionar la contratación del proveedor (Granados, 2025).

En otra línea, la implementación de gestiones administrativas digitales a nivel de Registro Nacional, municipalidades, entre otras entidades como PROCOMER con la plataforma

CrearEmpresa, todas mantienen una limitante en común, la necesidad de una firma digital para poder utilizarlas. Esto ha generado una exclusión sistemática de los administrados que no poseen dicha herramienta y que por lo tanto incurren en tramitar presencialmente, contraviniendo totalmente el principio de accesibilidad universal. También están las plataformas como COSEVI, Poder Judicial y Caja Costarricense del Seguro Social, las cuales brindan un servicio digital sin necesidad de firma digital, no obstante, para poder acceder a ellas se necesita realizar una gestión inicial presencial, la cual consiste por medio de la cédula y la verificación de un correo electrónico para dar un acceso inicial a su sistema.

1.4. Justificación del tema

La presente investigación se justifica en brindar un análisis sobre la digitalización en la gestión administrativa, enfocado en los principios generales de la Administración Pública, protección de datos y accesibilidad digital. Esto debido a la imperiosa necesidad de que se brinde un marco normativo sólido, coherente y consistente que facilite la implementación de herramientas digitales en el sistema estatal, sino que también brinde seguridad jurídica y proteja los derechos fundamentales de los individuos que lo utilizan, como el derecho a la autodeterminación informativa, a la intimidad, secreto de las comunicaciones o al consentimiento informado, por ejemplo.

La digitalización de la conducta administrativa no sólo debe ser considerada como una simple actualización del sistema operativo de un dispositivo como una computadora o teléfono inteligente, sino que es un proceso que debe implementarse desde la norma con base al principio de legalidad que rige el Derecho Administrativo, por lo que se requiere de una revisión normativa y doctrinal, que pueda conciliar los fundamentos clásicos de la materia con los retos y las oportunidades que el ambiente digital puede ofrecer. Debido a esto, se vela por una justificación

de contribución teórica y práctica que pueda ser beneficiosa en la práctica institucional pública, sirviendo como guía para futuras modificaciones normativas o rediseños operativos en la Administración Pública.

Desde un enfoque de relevancia social, lo que esta investigación busca es sensibilizar la necesidad de la adaptación de la Administración Pública a las exigencias de la rápida evolución de una sociedad cada vez más interconectada, el desarrollo tecnológico y la globalización. En ese sentido, se reflexiona sobre como el acceso, el manejo del internet y el uso generalizado de dispositivos tecnológicos que han redefinido las formas de interacción entre la ciudadanía y el Estado, abriendo nuevas oportunidades para la inclusión y participación, pero también exponiendo vulnerabilidades en relación con la ciberseguridad, homogeneidad de plataformas de acceso y el manejo de información de las cuales la Administración Pública debe solventar lo más pronto posible.

1.5. Objetivos

1.5.1. Objetivo General

Analizar el Derecho Administrativo Digital costarricense basado en su marco normativo y en el derecho comparado para la implementación a través de propuestas.

1.5.2. Objetivos Específicos

- **Compilar** el marco normativo costarricense aplicable a la digitalización en la administración pública.
- **Estimar** basado en el marco normativo avances sobre gobernanza digital, infraestructura tecnológica, protección de datos, identidad digital e interoperabilidad administrativa**.**

- **Comparar** el marco normativo nacional con dos modelos normativos avanzados en el tema de digitalización de la Administración Pública.
- **Considerar** propuestas de implementación a través de cambios en la normativa.

1.6. Alcances

Esta investigación se centra en un análisis normativo de la digitalización de la Administración Pública en general, como una herramienta eficaz en la gestión administrativa, del cual tiene como alcance principal la identificación de las ventajas, oportunidades y desafíos que presenta la normativa vigente. Con base al desarrollo de la investigación, se busca generar un antecedente nacional donde se refleje la urgencia de implementar un marco normativo basado en leyes consolidadas ante la rápida evolución de la tecnología frente el Derecho Administrativo. Esto debido a que se ha quedado desactualizado y que a corto plazo puede generar problemáticas en querer implementar la tecnología de una forma más rápida.

1.7. Limitaciones

El trabajo de investigación se encuentra inmerso en una serie de limitaciones. En primer lugar, debido a la amplitud normativo relacionado con tecnología, digitalización y protección de datos, que también involucra a sujetos de Derecho Privado, se requiere de una selección material de normativa que cumpla con las necesidades y disposiciones acordes a los objetivos de investigación, y más que todo que sean aplicables al Derecho Público.

Asimismo, al ser la presente investigación sobre la Administración Pública en general y la misma es bastante amplia, con diferentes instituciones de gobierno central, organismo centralizados, descentralizados, desconcentrados, autónomos y gobiernos locales, por mencionar

algunos de ellos; se debe limitar a lo general, ya que hay muchos casos puntuales que pueden ser objeto de estudio por sí mismo.

Por otro lado, la investigación se encuentra sujeta a un periodo académico específico, por lo que debe acogerse a fechas previamente estipuladas por la institución educativa, por lo que impide un análisis con mayor plazo sobre el impacto de la normativa más reciente, como la creación de Agencia Nacional de Gobierno Digital o la Identidad Digital Costarricense del Tribunal Supremo de Elecciones.

Además, el tema y el enfoque dado en el trabajo de investigación no se ha desarrollado recientemente a nivel nacional, por lo que la información doctrinal e investigativa es sesgada a trabajos de carácter internacional en su gran mayoría.

1.8. Marco Metodológico

El enfoque que se ha aplicado para realizar esta investigación es el cualitativo, ya que su estructura comprende:

> El propósito y objetivo(s). (…) La justificación y la viabilidad. Una exploración de las deficiencias en el conocimiento del problema. La definición inicial del ambiente o contexto donde se realizará la investigación. Todo lo anterior en relación con el fenómeno o problema central de interés; es decir, el propósito, finalidad u objetivo debe colocar la atención en la idea fundamental de la investigación. (Hernández Sampieri et al, p. 413)

Así mismo Barrantes (2014, pp. 86, 95) indica que el enfoque cualitativo se fundamenta en la metodología interpretativa, la cual se centra en el descubrimiento de conocimiento y el manejo de datos es utilizado de forma explicativa.

Debido a lo anterior, el manejo de la información adquirida se interpreta y analiza desde una perspectiva normativa, centrada en las temáticas que la investigación busca fundamentar a

partir de la normativa vigente, tanto nacional como internacional, así como de la doctrina, los datos recopilados y las entrevistas realizadas. Esto difiere del enfoque cuantitativo, que se desarrolla mediante instrumentos objetivos y confiables, utilizando técnicas estadísticas para el análisis de datos y la generalización de resultados, donde el investigador se mantiene ajeno al objeto de estudio (Barrantes, 2014, p. 94). En cambio, en la interpretación jurídica, el investigador se encuentra directamente inmerso en el campo de estudio por lo cual el enfoque más adecuado es el cualitativo.

Con base en el objetivo de la investigación, esta se clasifica como explicativa, puesto que, tal como lo define Barrantes (2014, p. 86), se orienta a "explicar los fenómenos y el estudio de sus relaciones para conocer su estructura y los aspectos que intervienen en su dinámica". En este caso, se pretende analizar cómo la normativa vigente relacionada con la digitalización ha sido implementada en el marco de la Administración Pública, identificando los desafíos y oportunidades existentes, con el fin de brindar recomendaciones fundamentadas en la doctrina y en el derecho comparado con normativa internacional.

1.9. Fuentes de información

1.9.1. Fuentes primarias de información

Hernández-Sampieri et al (2006, p.66) define a las fuentes primarias como "el objeto de la investigación bibliográfica o revisión de la literatura y proporcionan datos de primera mano; pues se trata de documentos que contienen los resultados de los estudios correspondientes", las cuales para esta investigación se consideran a las leyes que constituyen el ordenamiento jurídico nacional, entre ellas se encuentra la Constitución Política de la República de Costa Rica, Ley General de Administración Pública, Ley de Protección de la Persona frente al tratamiento de sus datos

personales; así como otras leyes, reglamentos, decretos ejecutivos. Se tendrá en cuenta la aplicación de convenios internacionales y de la normativa proveniente de países extranjeros, atendiendo a su jerarquía dentro del sistema de leyes y reglamentos pertinentes a la temática investigativa.

1.9.2. Fuentes secundarias de información

Se entiende por fuentes secundarias aquellas que reelaboran o interpretan la información obtenida directamente de fuentes primarias dentro de un área específica del conocimiento (Hernández-Sampieri et al, 2006, p.66). Se considerarán como fuentes secundarias el uso de recursos como los artículos especializados, doctrina nacional e internacional, planes de trabajo, monografías, videos, conversatorios relacionados con la digitalización de las gestiones administrativas, así como jurisprudencia de relevancia.

1.10. Resumen

En el primer capítulo se desarrollan los aspectos inmersos para el desarrollo del trabajo investigativo desde el planteamiento del problema a tratar, la problematización y la justificación del por qué se quiere abarcar el tema en concreto. Esto se acompaña con los objetivos, tanto generales como específicos que se quieren alcanzar en esta investigación, así como sus alcances y limitaciones. En relación con el Marco Metodológico se estipula un enfoque cualitativo desde una perspectiva interpretativa y explicativa, donde además se indican las fuentes primarias y secundarias de la información a recopilar para el desarrollo de los siguientes capítulos.

Seguidamente, el capítulo segundo consiste en el Marco Teórico. Su primer punto es el marco conceptual, donde se definen conceptos de relevancia para la comprensión del análisis como “acto administrativo digital”, “datos biométricos”, “firma digital”, “interoperabilidad”, entre otros.

Posteriormente se hará referencia a comprender los siguientes ejes de análisis como el acto administrativo desde la digitalización, el término de gestión administrativa digital y este mismo como un servicio público.

Como tercer capítulo, se encuentre el Marco Normativo. En el cual se desarrolla la normativa vigente aplicable a la digitalización desde la Administración Pública, donde se menciona la carta magna de la Constitución Política, La Ley General de Administración Pública, las cuales son pilares dentro del principio de legalidad, así como otras leyes, decretos ejecutivos y reglamentos relacionados a la temática.

El capítulo cuarto desenvuelve el análisis de resultado en base al marco teórico y normativo plasmado en el capítulo anteriormente señalado desde diferentes puntos específico como la gobernanza estructural, infraestructura, protección de datos, entre otros; posteriormente se determinará una serie de oportunidades y desafíos a raíz de este mismo análisis. Asimismo, se abarca el análisis de derecho comparado en los países de Estonia y Chile, los cuales se seleccionaron debido su desarrollo de la gestión digital en la Administración Pública. Como última instancia se plantean propuestas y recomendaciones para la consolidación del Derecho Administrativo Digital en Costa Rica. El último capítulo de esta investigación abarca las conclusiones a las que se pudo llegar con esta investigación y las recomendaciones planteadas desde un enfoque prospectivo en compañía de las referencias bibliográficas.

A modo de corolario, el primer capítulo de este trabajo de investigación define y delimita el problema de investigación, justificar su relevancia jurídica y social, y fijar con claridad los objetivos, alcances y límites del estudio, evidenciando que la digitalización de la Administración Pública no puede abordarse únicamente desde una perspectiva técnica u operativa, sino que exige una reflexión jurídica profunda, sistemática y coherente con los principios estructurales del

Derecho Administrativo. Además, los antecedentes evolución histórica, el análisis del contexto normativo costarricense y la problematización planteada revelan una tensión latente entre el avance acelerado de la tecnología y un marco jurídico que aún no logra integrarla de manera armónica. En este sentido, el siguiente capítulo se orienta a construir el Marco Teórico de la investigación, desarrollando un marco conceptual y doctrinal que servirá como base analítica indispensable para el estudio del Derecho Administrativo Digital.

CAPITULO II – MARCO TEÓRICO

El presente capítulo tiene como propósito fundamental establecer el soporte conceptual y doctrinal que sustenta la investigación, delimitando los ejes teóricos del Derecho Administrativo Digital en el contexto costarricense. Para ello, se abordará la evolución de la función administrativa frente al fenómeno de la transformación digital. Este desarrollo teórico no solo permitirá comprender la naturaleza jurídica de la digitalización en la Administración Pública, sino que servirá de base para comparar la eficacia del sistema normativo nacional frente a modelos internacionales de vanguardia.

2.1. Marco Conceptual

2.1.1. Accesibilidad Digital

En primer lugar, se debe establecer una definición de accesibilidad desde un ámbito general, del cual la normativa costarricense ha desarrollado de manera amplia y se evidencia en la Ley de Igualdad de Oportunidades para las Personas con Discapacidad N°7600:

> Accesibilidad: Son las medidas adoptadas, por las instituciones públicas y privadas, para asegurar que las personas con discapacidad tengan acceso, en igualdad de condiciones con

> los demás, al entorno físico, el transporte, la información y las comunicaciones, incluidos los sistemas y las tecnologías de la información y las comunicaciones y a otros servicios e instalaciones abiertos al público o de uso público. Estas medidas incluyen también la identificación y eliminación de dichas barreras. (Ley 7600, 1996, Art. 2)

A pesar de que esta definición permite entender de una manera amplía la accesibilidad, para objeto de la presente investigación es necesario una delimitación más centrada en el área digital, la UC Berkeley lo define como: "digital accessibility means that websites, tools, and technologies are designed and developed so that people with disabilities can use them." (UC Berkeley, s.f.).

Por lo que se puede concluir, que la accesibilidad digital es aquel diseño y desarrollo aplicado a los entornos digitales que permiten a las personas con alguna discapacidad utilizar páginas web, herramientas y tecnologías digitales de manera simple y acorde a las limitaciones personales individuales, concediendo a toda la población el uso de dichos entornos digitales y suprimiendo la discriminación.

2.1.2. Acto Administrativo Digital

De igual manera, la definición de acto administrativo, la Ley General de Administración Pública en sus artículos 128 y siguientes esboza someramente su definición dentro de la normativa costarricense. Ante este presente capítulo teórico, se menciona los artículos 128 y 130 que determinan que "Será válido el acto administrativo que se conforme sustancialmente con el ordenamiento jurídico, incluso en cuanto al móvil del funcionario que lo dicta." (Ley General De Administración Pública, 1978, Art. 128) y que "deberá aparecer objetivamente como una manifestación de voluntad libre y consciente, dirigida a producir el efecto jurídico deseado para el fin querido por el ordenamiento" (Ley General De Administración Pública, 1978, Art. 130).

A manera de análisis se determina que un acto administrativo es aquel acto que produce la administración de acuerdo con el Derecho Administrativo con el fin de producir un efecto jurídico ya establecido en la normativa. Además, la Procuraduría General de la República en el dictamen C-082-91, señala que cualquier acto que emita la Administración Pública en referencia a temas que se encuentren regulados por el Derecho Privado no pueden ser considerados un acto administrativo, solo los que respondan a Derecho Público, precisamente al Administrativo.

Por lo tanto, un acto administrativo digital es "aquella declaración de voluntad formulada por un sujeto de la Administración Pública en ejercicio de una potestad administrativa, que es emitida o notificada a través de medios electrónicos." (Acceso a la Justicia, s.f.). Señalado lo anterior, se debe hacer la aclaración que para motivos de este trabajo investigativo en vez de electrónicos debe de entenderse digitales.

2.1.3. Administración Pública

La Ley General de la Administración Pública en el artículo 1 establece que la Administración Pública esta "constituida por el Estado y los demás entes públicos, cada uno con personalidad jurídica y capacidad de derecho público y privado." (Ley General de la Administración Pública, Artículo 1). Definición que de unirse con la del Diccionario Panhispánico de la Real Academia Española que la define como el "Conjunto de órganos y entidades que, encuadrados en el gobierno estatal, autonómico o local, sirven con objetividad los intereses generales ejecutando las leyes y prestando los servicios públicos correspondientes." (Diccionario panhispánico del español jurídico, s.f., Administración Pública)

Se debe subrayar la importancia de la estructura organizativa del Estado y otros entes públicos. Esta estructura no solo posee personalidad jurídica, sino también la capacidad de actuar tanto en el ámbito del derecho público como en el privado. Esto implica que la Administración

Pública tiene la facultad de tomar decisiones y ejecutar acciones que afectan tanto a la esfera pública como a la privada, siempre con el objetivo de servir los intereses generales y garantizar el cumplimiento de las leyes.

Además, la Administración Pública desempeña un papel crucial en la prestación de servicios públicos. Estos servicios son esenciales para el bienestar de la sociedad y abarcan una amplia gama de áreas, desde la educación y la salud hasta la seguridad y el transporte. La capacidad de la Administración Pública para ejecutar estos servicios de manera eficiente y objetiva es fundamental para el desarrollo y la estabilidad de cualquier Estado. En este sentido, la Administración Pública no solo actúa como un ejecutor de leyes, sino también como un facilitador del desarrollo social y económico, asegurando que los recursos y servicios lleguen a todos los ciudadanos de manera equitativa y justa.

2.1.4. Autodeterminación informativa

La autodeterminación informativa es la "Garantía de la persona física o jurídica a conocer lo que conste acerca de ella, sus bienes o derechos en cualquier registro o archivo, de toda naturaleza, sea mecánica, electrónica o informatizada, pública o privada." (Diccionario Usual del Poder Judicial, s.f.).

La autodeterminación informativa no solo representa el derecho de cada individuo a conocer, controlar y decidir sobre el uso de sus datos personales, sino que también implica una facultad activa de gestión sobre la información que lo identifica. Este principio se rige como una garantía fundamental en el entorno digital, donde la recopilación masiva de datos por parte de entidades públicas y privadas puede poner en riesgo la privacidad, la dignidad y la libertad de las personas. En este sentido, la autodeterminación informativa exige que cualquier tratamiento de

datos personales se realice con el consentimiento informado del titular, asegurando que este comprenda plenamente el propósito, alcance y consecuencias del uso de su información.

Además, la autodeterminación informativa se vincula estrechamente con otros principios jurídicos como legalidad, proporcionalidad y transparencia. En el marco del Derecho Administrativo Digital, este derecho cobra especial relevancia, ya que las gestiones administrativas modernas dependen cada vez más de plataformas tecnológicas que almacenan, procesan y comparten datos personales. Por ello, es indispensable que el ordenamiento jurídico establezca mecanismos claros para la protección de estos datos, involucrando a un conjunto de derechos como el acceso, rectificación, cancelación y oposición, así como la obligación de las instituciones de garantizar la seguridad, confidencialidad y trazabilidad de la información. La autodeterminación informativa, entonces, no solo protege al individuo, sino que también fortalece la confianza ciudadana en el uso de tecnologías por parte del Estado.

2.1.5. Big data

La *Big Data* o macrodatos se refiere al conjunto masivo de datos que por su tamaño y complejidad no pueden ser procesados de manera tradicional y que solo gracias a la capacidad de almacenamiento actual pueden ser tratados para su análisis, identificación de patrones y hasta predicción de comportamiento.

La *Big Data* "incluyen datos estructurados, como una base de datos de inventario o una lista de transacciones financieras; datos no estructurados, como publicaciones sociales o videos; y conjuntos de datos mixtos" (Chen, 2024). Los datos deben de contar con las cinco "V" de la *big data* que son: volumen, velocidad, variedad, veracidad y valor. Además, el autor estima que la *big data* usada en el área de la Administración Pública puede:

> (...)pueden recopilar datos de muchas fuentes diferentes (...) Esto puede impulsar la eficiencia de muchas formas distintas, como detectar las tendencias de los conductores para optimizar la gestión de los cruces y asignar mejor los recursos en las escuelas. Los gobiernos también pueden publicar datos públicamente, lo que permite una mayor transparencia para reforzar la confianza pública. (Chen, M., 2024)

En síntesis, la *Big Data* puede definirse como el conjunto masivo de datos estructurados y no estructurados que, por su volumen, velocidad y variedad, requieren de tecnologías avanzadas para su procesamiento, análisis y aprovechamiento. Esta definición no solo contempla la dimensión técnica del fenómeno, sino también su capacidad para generar valor a partir de la información, permitiendo identificar patrones, predecir comportamientos y tomar decisiones informadas en tiempo real. En el contexto de la Administración Pública, esta herramienta se convierte en un recurso estratégico para la mejora de la eficiencia institucional y la formulación de políticas públicas basadas en evidencia.

2.1.6. Ciberseguridad

"La ciberseguridad es la práctica de proteger equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales." (Amazon Web Services, s.f.). En el contexto de la Administración Pública, la ciberseguridad adquiere una relevancia crítica, ya que las instituciones estatales manejan información sensible de los ciudadanos, como datos personales, financieros, de salud y otros registros que deben ser resguardados con altos estándares de seguridad.

La importancia de aplicar ciberseguridad en la gestión pública radica en la necesidad de garantizar la confidencialidad, integridad y disponibilidad de la información. Un sistema público vulnerable puede ser blanco de ciberataques que comprometan no solo la privacidad de los

ciudadanos, sino también la operatividad de servicios esenciales como salud, justicia o recaudación fiscal. Además, la digitalización de trámites administrativos exige que las plataformas tecnológicas sean seguras, confiables y resistentes a amenazas, para fomentar la confianza ciudadana en el uso de servicios digitales.

Implementar medidas de ciberseguridad en la Administración Pública también permite cumplir con principios jurídicos fundamentales como el principio de legalidad, la protección de datos personales y la autodeterminación informativa. Esto implica establecer protocolos de autenticación robustos, sistemas de respaldo, monitoreo constante de amenazas y una gobernanza clara sobre el uso y tratamiento de la información. En definitiva, la ciberseguridad no solo es una herramienta técnica, sino un pilar esencial para la modernización del Estado y la defensa de los derechos fundamentales en la era digital.

2.1.7. Cloud computing

El cloud computing o computación en la nube es el acceso a servicios bajo demanda de servicios informáticos mediante una conexión de internet, estos pueden ser servidores físicos o virtuales, almacenamiento de datos, desarrollo de aplicaciones, software, plataformas analíticas, inteligencia artificial y demás.

El cloud computing “permite almacenar y procesar enormes volúmenes de datos a gran velocidad: más capacidad de almacenamiento y computación de la que la mayoría de las organizaciones pueden o quieren adquirir e implementar en sus propias instalaciones.” (Susnjara & Smalley, s.f.) por lo que es una alternativa que mejora la rentabilidad, la agilidad y el valor estratégico de la organización que lo utiliza incluso tiene la capacidad de escalar según la necesidad del usuario.

En este contexto, el cloud computing se presenta como una herramienta clave para la transformación digital del Estado, al permitir una gestión más eficiente, segura y flexible de los recursos tecnológicos. Su implementación en la Administración Pública no solo optimiza el almacenamiento y procesamiento de datos, sino que también facilita la interoperabilidad entre instituciones, la automatización de procesos y la prestación de servicios públicos en línea. Esto se traduce en una mejora significativa en la atención ciudadana, al reducir los tiempos de respuesta, eliminar trámites presenciales innecesarios y garantizar el acceso continuo a los servicios, incluso en situaciones de emergencia o alta demanda.

No obstante, para que el uso del cloud computing sea realmente efectivo en el sector público, es indispensable contar con un marco jurídico y técnico robusto que regule su aplicación. La protección de datos personales, la ciberseguridad, la neutralidad tecnológica y la interoperabilidad deben ser pilares fundamentales en esta transición. Además, se requiere una planificación estratégica que contemple la capacitación del personal, la inversión en infraestructura digital y la creación de políticas públicas que promuevan la inclusión tecnológica. Solo así se podrá garantizar que la computación en la nube no solo modernice la gestión administrativa, sino que también fortalezca la confianza ciudadana en el uso de tecnologías digitales por parte del Estado.

2.1.8. Compliance

El compliance es un “conjunto de procedimientos y buenas prácticas adoptados por las organizaciones para identificar y clasificar los riesgos operativos y legales a los que se enfrentan y establecer mecanismos internos de prevención, gestión, control y reacción frente a los mismos.” (World Compliance Association, s.f.).

A pesar de que el compliance ha sido tradicionalmente desarrollado en el ámbito corporativo, su aplicación en el sector público resulta cada vez más pertinente ante los desafíos

que plantea la digitalización de la gestión administrativa. La incorporación de mecanismos de cumplimiento normativo en las instituciones estatales permite establecer controles internos que aseguren la legalidad, la transparencia y la rendición de cuentas, especialmente en contextos donde el uso de tecnologías puede generar riesgos jurídicos, éticos y operativos. En este sentido, el compliance se convierte en una herramienta estratégica para prevenir irregularidades, fortalecer la cultura institucional y garantizar que las actuaciones administrativas se ajusten a los principios del Derecho Público.

Desde la perspectiva del Derecho Administrativo, el compliance puede ser entendido como un complemento a los principios de legalidad, proporcionalidad y responsabilidad funcional. Su implementación no implica una sustitución de los controles tradicionales, sino una evolución hacia modelos de gobernanza más proactivos y adaptativos, capaces de responder a los riesgos emergentes del entorno digital. La adopción de programas de compliance en la Administración Pública costarricense podría contribuir a una mayor estandarización de procesos, mejorar la interoperabilidad entre instituciones y asegurar que la transformación digital se desarrolle dentro de un marco jurídico sólido, ético y orientado al interés público.

2.1.9. Cookies

Las cookies son “archivos de texto con pequeños datos, como un nombre de usuario y contraseña, que se utilizan para identificar tu ordenador cuando utilizas una red.” (Kaspersky, s.f.) actualmente y debido a regulaciones internacionales como el Reglamento General de Protección de Datos de la Unión Europea y la Ley de Privacidad del Consumidor de California los sitios web deben solicitar permiso de uso en las visitas al sitio.

El uso que se da actualmente a las cookies es para que “los navegadores web rastreen, personalicen y guarden información acerca de la sesión de cada usuario”, estos con el fin de

gestionar la sesión del usuario que visita la página proporcionando una personalización sobre el contenido que se despliega dirigido específicamente a ese usuario, de la misma manera puede rastrear varios datos analíticos de rendimiento de las sesiones.

En el contexto de la Administración Pública, las cookies pueden convertirse en herramientas útiles para mejorar la experiencia del administrado en plataformas digitales estatales. Al permitir el almacenamiento de preferencias, historial de navegación y datos de sesión, las instituciones públicas pueden personalizar los servicios ofrecidos, agilizar trámites y facilitar el acceso a información relevante. Por ejemplo, al utilizar cookies, un sistema de gestión tributaria podría recordar los formularios previamente completados por el usuario, evitando la necesidad de ingresar repetidamente los mismos datos. Sin embargo, este uso debe estar estrictamente regulado para garantizar la protección de la privacidad y la seguridad de la información personal, respetando principios como la autodeterminación informativa y la protección ante el tratamiento de datos.

Es importante diferenciar las cookies de los metadatos, ya que, aunque ambos se relacionan con la información digital, cumplen funciones distintas. Las cookies son archivos creados por los sitios web que almacenan datos sobre la interacción del usuario con la página, como preferencias de idioma, servicios vistos o credenciales de acceso. En cambio, los metadatos son datos que describen otros datos, como la fecha de creación de un documento, el autor, la ubicación geográfica de una fotografía o el tipo de archivo. Mientras las cookies se centran en la experiencia del usuario en la web, los metadatos son esenciales para la organización, búsqueda y trazabilidad de la información en sistemas digitales, incluyendo los utilizados por la Administración Pública.

En conclusión, las cookies representan una herramienta tecnológica que, bien utilizada, puede optimizar la relación entre el ciudadano y el Estado en entornos digitales. No obstante, su implementación debe estar acompañada de un marco jurídico sólido que garantice la transparencia,

la protección de datos personales y el respeto por los derechos fundamentales. La comprensión clara de su funcionamiento, así como su diferenciación con otros conceptos como los metadatos, es esencial para avanzar hacia una gestión administrativa digital responsable, eficiente y centrada en el usuario.

2.1.10. Datos biométricos

Los datos biométricos "son los datos personales relativos a las características únicas del ser humano, sean físicas, fisiológicas o asociadas al comportamiento, que faciliten y garanticen la identificación de un individuo (persona física), mediante sistemas o procedimientos tecnológicos." (Monforte, E., s.f.)

Los datos biométricos son información personal que se refiere a las características únicas e intransferibles de cada individuo, como huellas dactilares, rasgos faciales, iris, voz, o patrones de comportamiento. Estas características permiten identificar de manera precisa a una persona mediante sistemas tecnológicos avanzados, lo que los convierte en herramientas clave en la era digital.

En la Administración Pública, los datos biométricos se utilizan para autenticar la identidad de los ciudadanos en trámites digitales, como el acceso a portales gubernamentales, la firma de documentos electrónicos, y la gestión de servicios como salud, justicia o tributación. Por ejemplo, en Costa Rica, el Sistema de Verificación de Identidad (VID) del Tribunal Supremo de Elecciones permite cotejar huellas digitales con las registradas en su base de datos, facilitando la identificación segura de los usuarios en procedimientos administrativos. Esta tecnología reduce el riesgo de suplantación de identidad y agiliza los procedimientos, eliminando la necesidad de trámites presenciales.

El acceso a portales digitales mediante autenticación biométrica representa un avance significativo en términos de seguridad y comodidad para los ciudadanos. Plataformas estatales que integran mecanismos como la huella digital o el reconocimiento facial permiten una interacción más directa y segura con la Administración Pública. No obstante, es fundamental que estas tecnologías se implementen con criterios de equidad, accesibilidad y transparencia, considerando a poblaciones vulnerables que podrían enfrentar barreras tecnológicas, como adultos mayores o personas con discapacidad.

En conclusión, los datos biométricos son una herramienta poderosa para la modernización de la gestión administrativa, pero su uso debe estar acompañado de una regulación clara y garantista. La digitalización del Derecho Administrativo no solo implica adoptar nuevas tecnologías, sino también repensar los principios jurídicos que rigen la relación entre el ciudadano y la Administración Pública. Solo mediante un enfoque equilibrado entre innovación y protección de derechos fundamentales se podrá consolidar un modelo de gobierno digital inclusivo, seguro y eficiente.

2.1.11. E-Government (Gobierno Electrónico)

El e-goverment o gobierno electrónico se puede definir como “el uso de las TIC [sic] para brindar servicios gubernamentales a la ciudadanía y a las empresas de manera más eficaz y eficiente.” (Naciones Unidas, s.f.). El gobierno electrónico no solo implica la digitalización de trámites, sino también una transformación profunda en la forma en que el Estado se relaciona con la ciudadanía. A través del uso de tecnologías de la información y la comunicación (TIC), se busca mejorar la eficiencia institucional, reducir la burocracia y aumentar la transparencia en la gestión pública. Esto permite que los ciudadanos accedan a servicios gubernamentales de manera remota,

rápida y segura, lo que resulta especialmente relevante en contextos de emergencia o para poblaciones con acceso limitado a oficinas físicas.

Además, el e-government promueve la interoperabilidad entre instituciones, facilitando el intercambio de información y evitando la duplicidad de trámites. Iniciativas como los portales únicos de servicios, la firma digital, los expedientes electrónicos y los sistemas de autenticación ciudadana son ejemplos de cómo se puede consolidar una administración pública más moderna, inclusiva y centrada en el usuario. Sin embargo, para que estas herramientas sean efectivas, es indispensable contar con un marco normativo sólido, políticas públicas claras y una infraestructura tecnológica adecuada.

El e-government representa una oportunidad estratégica para fortalecer la relación entre el Estado y la ciudadanía, optimizando los servicios públicos y promoviendo una gestión más transparente y eficiente. Su implementación debe ir acompañada de una visión integral que contemple aspectos técnicos, jurídicos y sociales, asegurando que la digitalización beneficie a toda la población sin generar nuevas brechas de acceso o exclusión.

2.1.12. Entity list

La Entity List o lista de entidades, publicada por primera vez en el año de 1997, es una lista que "identifica personas o direcciones de personas que se cree razonablemente que están involucradas, o que representan un riesgo significativo de estar o llegar a estar involucradas, en actividades contrarias a los intereses de seguridad nacional o de política exterior de los Estados Unidos." (Oficina de Industria y Seguridad, s.f.).

Esta lista tiene como objetivo restringir el acceso de las entidades incluidas a productos, software y tecnologías de origen estadounidense, especialmente aquellas que podrían ser utilizadas para fines militares, de vigilancia o que representen un riesgo estratégico.

Desde una perspectiva de Derecho Internacional, la inclusión en la Entity List implica la imposición de controles de exportación que requieren licencias específicas para la transferencia de bienes y servicios hacia las entidades señaladas. Esta medida no solo tiene implicaciones comerciales, sino que también puede afectar la cooperación científica, tecnológica y académica entre países.

En el contexto de la digitalización y el Derecho Administrativo, la Entity List representa un desafío para las Administraciones Públicas que buscan implementar tecnologías extranjeras en sus sistemas públicos, ya que deben considerar las restricciones internacionales vigentes y evaluar el impacto legal, ético y de seguridad que conlleva la adopción de soluciones tecnológicas provenientes de entidades sancionadas.

2.1.13. Expediente Digital

Los expedientes digitales son “conjuntos de documentos digitales que son organizados y gestionados de manera estructurada a través de sistemas informáticos.” (Digital Ware, s.f.). En Costa Rica, la Ley N°8220 de “Protección al ciudadano del exceso de requisitos y trámites administrativos” permite la creación de expedientes digitales para las gestiones administrativas que se manejen por este medio. Además, el país cuenta actualmente con varios expedientes digitales de acceso mediante autenticación como el del Poder Judicial y la Caja Costarricense del Seguro Social.

En este contexto, el expediente digital se consolida como una herramienta clave para la modernización de la gestión administrativa en la Administración Pública. Su implementación permite la organización estructurada de documentos electrónicos, facilitando el acceso, la trazabilidad y el seguimiento de los trámites en tiempo real. A través de sistemas informáticos seguros y plataformas interoperables, el expediente digital no solo agiliza los procedimientos

internos de las instituciones, sino que también mejora la experiencia del administrado al ofrecerle mayor transparencia, eficiencia y comodidad en la interacción con el Estado.

En definitiva, el expediente digital no representa únicamente una transformación tecnológica, sino una evolución sustantiva en la forma de concebir y ejecutar la función administrativa. Al garantizar la autenticidad, integridad y disponibilidad de la información, esta herramienta fortalece la seguridad jurídica y promueve una gestión pública más eficiente, inclusiva y centrada en el ciudadano. Su consolidación como instrumento normativo y operativo es indispensable para avanzar hacia un modelo de gobierno digital que responda con eficacia a las exigencias de una sociedad cada vez más interconectada.

2.1.14. Firma Digital

La firma digital "es una herramienta tecnológica que permite verificar su integridad, así como identificar jurídicamente la vinculación de forma clara al autor con el documento electrónico." (Banco Central de Costa Rica, s.f.)

Regulada en Costa Rica por la Ley N.º 8454 "Ley de Certificados, Firmas Digitales y Documentos Electrónicos", se establece un marco normativo robusto que garantiza la autenticidad, integridad y no repudio de los documentos firmados digitalmente, equiparando su validez legal a la de los documentos físicos firmados de manera manuscrita. Además, la ley contempla principios como la neutralidad tecnológica, la interoperabilidad y la regulación mínima, lo que permite su aplicación en diversos ámbitos del Derecho Público y Privado.

En el contexto de las gestiones administrativas en Costa Rica, la firma digital ha sido implementada como un mecanismo para agilizar trámites, reducir el uso de papel y fortalecer la seguridad jurídica en las actuaciones de la Administración Pública. Instituciones como el Poder

Judicial, la Caja Costarricense del Seguro Social y el Registro Nacional han adoptado sistemas que permiten la autenticación de usuarios y la firma de documentos mediante esta tecnología. Por consiguiente, la firma digital facilita la interoperabilidad entre instituciones, permitiendo que los ciudadanos realicen trámites en línea sin necesidad de presentar físicamente documentos firmados, lo que mejora la eficiencia y accesibilidad de los servicios públicos.

En conclusión, la firma digital representa un avance significativo en la modernización del Estado costarricense, al permitir una gestión administrativa más eficiente, transparente y segura. No obstante, su implementación debe ir acompañada de políticas inclusivas que garanticen el acceso equitativo a esta tecnología, especialmente para poblaciones vulnerables que aún enfrentan barreras tecnológicas. La consolidación de la firma digital como instrumento jurídico y operativo en la Administración Pública es clave para fortalecer el principio de legalidad y promover una transformación digital coherente con los derechos fundamentales de los ciudadanos.

2.1.15. Hardware

El hardware "son los componentes físicos que componen un sistema informático y le permiten realizar funciones esenciales, como entrada, salida, procesamiento y almacenamiento." (IBM, s.f.) Ejemplos comunes incluyen el procesador (CPU), la memoria RAM, discos duros, unidades de estado sólido (SSD), tarjetas gráficas, monitores, teclados, impresoras y servidores.

En el contexto de la Administración Pública, el hardware no solo permite la operación de sistemas informáticos, sino que también constituye la base sobre la cual se ejecutan las plataformas digitales que brindan servicios a los ciudadanos.

La importancia de contar con un hardware adecuado en el sector público radica en su capacidad para garantizar la continuidad, eficiencia y seguridad de las gestiones administrativas.

Un equipo obsoleto o insuficiente puede generar fallos en los sistemas, pérdida de información, lentitud en los trámites y vulnerabilidades en la ciberseguridad.

Por ende, la modernización de los dispositivos físicos se debe a su integración con tecnologías emergentes como la computación en la nube, la virtualización de servidores y el uso de dispositivos inteligentes. Esta transformación permite una mayor escalabilidad, interoperabilidad y eficiencia energética.

En conclusión, el hardware es un pilar fundamental en la digitalización de la gestión administrativa. Su correcta implementación y actualización permiten que la Administración Pública cumpla con los principios de eficiencia, continuidad y accesibilidad, fortaleciendo la confianza ciudadana en los servicios digitales del Estado. La inversión en infraestructura tecnológica debe ser vista como una estrategia jurídica y operativa que garantice el cumplimiento de los derechos fundamentales en entornos digitales, especialmente en una sociedad cada vez más interconectada.

2.1.16. Inteligencia Artificial

La inteligencia Artificial o IA, se puede definir de dos maneras, la primera como su campo de estudio "relacionado con la creación de computadoras y máquinas que pueden razonar, aprender y actuar de una manera que normalmente requeriría inteligencia humana o que involucra datos cuya escala excede lo que los humanos pueden analizar." (Google Cloud, s.f.) y la segunda relacionada a su campo operativo como:

> (…) un conjunto de tecnologías que se basan principalmente en el aprendizaje automático y el aprendizaje profundo, que se usan para el análisis de datos, la generación de predicciones y previsiones, la categorización de objetos, el procesamiento de lenguaje

natural, las recomendaciones, la recuperación inteligente de datos y mucho más. (Google Cloud, s.f.)

La inteligencia artificial ha encontrado aplicaciones en una variedad de campos en la actualidad. En el ámbito empresarial, se utiliza para optimizar procesos, mejorar la toma de decisiones y personalizar la experiencia del cliente. Por ejemplo, los sistemas de recomendación en plataformas de streaming y comercio electrónico analizan los patrones de comportamiento de los usuarios para ofrecer sugerencias personalizadas. En el sector de la salud, la IA se emplea para el diagnóstico de enfermedades, la predicción de brotes epidémicos y la personalización de tratamientos médicos. Además, en el campo de la educación, las plataformas de aprendizaje en línea utilizan algoritmos de IA para adaptar el contenido educativo a las necesidades individuales de los estudiantes.

En cuanto a la digitalización de la Administración pública, la IA tiene un potencial significativo para transformar la manera en que los gobiernos interactúan con los ciudadanos y gestionan sus recursos. Los chatbots y asistentes virtuales pueden mejorar la atención al ciudadano, proporcionando respuestas rápidas y precisas a consultas comunes. Asimismo, la IA puede automatizar procesos burocráticos, reduciendo el tiempo y los costos asociados con la gestión de documentos y la tramitación de solicitudes. En el ámbito de la seguridad, los sistemas de IA pueden analizar grandes volúmenes de datos para detectar patrones de comportamiento sospechoso y prevenir delitos.

En conclusión, la inteligencia artificial está revolucionando diversos sectores al ofrecer soluciones innovadoras y eficientes. Su implementación en la Administración pública no solo mejorará la eficiencia operativa, sino que también facilitará una interacción más transparente y efectiva entre los gobiernos y los ciudadanos. A medida que la tecnología continúe avanzando, es

fundamental que se adopten enfoques éticos y responsables para garantizar que los beneficios de la IA se distribuyan de manera equitativa y se minimicen los riesgos asociados.

2.1.17. Interoperabilidad

La interoperabilidad se refiere a la capacidad de diferentes sistemas, dispositivos o aplicaciones para comunicarse, intercambiar datos y utilizar la información de manera efectiva. Esta característica es esencial en un mundo cada vez más digitalizado, donde la integración de tecnologías diversas es crucial para el funcionamiento eficiente de organizaciones y gobiernos. Según IBM, la interoperabilidad permite que los sistemas trabajen juntos sin problemas, facilitando la colaboración y el intercambio de información entre diferentes plataformas y tecnologías (IBM, s.f.).

En la Administración Pública, la interoperabilidad juega un papel fundamental en la modernización de los servicios gubernamentales. Permite que las distintas entidades públicas compartan información y recursos de manera eficiente, eliminando la necesidad de duplicar esfuerzos y reduciendo los tiempos de respuesta. Por ejemplo, un sistema interoperable puede permitir que los datos de un ciudadano, como su información de salud, educación y seguridad social, sean accesibles a través de una única plataforma, mejorando la eficiencia y la calidad del servicio público.

Las ventajas de la interoperabilidad son numerosas. En primer lugar, mejora la eficiencia operativa al permitir que los sistemas compartan datos y recursos sin necesidad de intervención manual. Esto no solo reduce los costos operativos, sino que también minimiza los errores humanos. Además, la interoperabilidad facilita la toma de decisiones informadas, ya que los datos integrados y accesibles en tiempo real permiten a los responsables de la toma de decisiones tener una visión completa y precisa de la situación. También promueve la transparencia y la rendición de cuentas,

ya que los datos compartidos entre diferentes entidades pueden ser auditados y verificados de manera más efectiva.

En conclusión, la interoperabilidad es una característica esencial en la era digital, especialmente en el ámbito de la Administración Pública. Su capacidad para integrar sistemas y facilitar el intercambio de información mejora la eficiencia, reduce costos y promueve la transparencia. A medida que las tecnologías continúan evolucionando, la interoperabilidad se convertirá en un componente aún más crítico para garantizar que los sistemas y servicios públicos puedan adaptarse y responder a las necesidades cambiantes de la sociedad. Es fundamental que los gobiernos y las organizaciones adopten enfoques interoperables para maximizar los beneficios de la digitalización y asegurar un futuro más conectado y eficiente.

2.1.18. Metadatos

Los metadatos son datos que describen otros datos, proporcionando información esencial sobre su contenido, estructura y contexto. Según PowerData, los metadatos incluyen detalles como el autor, la fecha de creación, el formato del archivo y las restricciones de acceso, entre otros aspectos (PowerData, s.f.). Estos datos adicionales permiten una mejor organización, búsqueda y gestión de la información, facilitando su uso y reutilización en diversos contextos.

En la Administración Pública, los metadatos juegan un papel crucial en la gestión de documentos y la transparencia gubernamental. Permiten que los registros y documentos oficiales sean fácilmente accesibles y verificables, mejorando la eficiencia administrativa y la rendición de cuentas. Por ejemplo, los sistemas de gestión documental utilizan metadatos para clasificar y archivar documentos de manera que puedan ser recuperados rápidamente cuando se necesiten. Además, los metadatos ayudan a garantizar la integridad y autenticidad de los documentos, lo que es fundamental para la confianza pública en los proce administrativos.

Los posibles usos de los metadatos son amplios y variados. En el ámbito de la seguridad, los metadatos pueden ser utilizados para rastrear el acceso y las modificaciones a documentos sensibles, proporcionando un registro detallado de quién hizo qué y cuándo. En el campo de la salud, los metadatos pueden ayudar a gestionar grandes volúmenes de datos de pacientes, facilitando la búsqueda de información relevante y mejorando la atención médica. Además, en el sector educativo, los metadatos pueden ser utilizados para organizar y acceder a recursos educativos digitales, mejorando la experiencia de aprendizaje de los estudiantes.

En conclusión, los metadatos son una herramienta poderosa para la gestión de la información en la era digital. Su capacidad para describir y contextualizar otros datos mejora la eficiencia, la transparencia y la seguridad en diversos sectores, incluyendo la Administración Pública. A medida que la digitalización continúa avanzando, es esencial que las organizaciones y los gobiernos adopten prácticas efectivas de gestión de metadatos para maximizar los beneficios de la información digital y garantizar su uso responsable y ético.

2.1.19. Privacidad Digital

La privacidad digital se refiere al derecho de los usuarios a controlar cómo se recopilan y utilizan sus datos personales en internet. Esto incluye decidir qué información se comparte con terceros y qué datos se mantienen en privado. La privacidad digital abarca aspectos como la privacidad de la información, la privacidad de la comunicación y la privacidad individual, y es fundamental para proteger la información sensible que compartimos en línea (Husain, 2023).

En la Administración Pública, la privacidad digital juega un papel crucial en la protección de los datos personales de los ciudadanos. Las instituciones gubernamentales manejan grandes volúmenes de información sensible, como datos de salud, información financiera y registros personales. Es esencial que el Derecho Administrativo implemente políticas y tecnologías que

garanticen la seguridad y confidencialidad de estos datos. Como la implementación de sistemas de autenticación robustos y el uso de encriptación para proteger la información almacenada y transmitida son medidas fundamentales para asegurar la privacidad digital en el sector público.

Además de proteger los datos personales, la privacidad digital puede mejorar la transparencia y la confianza de los ciudadanos en los servicios gubernamentales. Al garantizar que la información personal se maneje de manera segura y responsable, los gobiernos pueden fomentar una mayor participación ciudadana y mejorar la eficiencia de los servicios públicos. Asimismo, la privacidad digital es esencial para cumplir con las regulaciones y normativas internacionales sobre protección de datos, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea.

En síntesis, la privacidad digital es un componente esencial en la era de la información. Su implementación en la Administración Pública no solo protege los datos personales de los ciudadanos, sino que también mejora la transparencia, la confianza y la eficiencia de los servicios gubernamentales. A medida que la tecnología continúa avanzando, es crucial que los gobiernos adopten políticas y prácticas que garanticen la privacidad digital, asegurando que los beneficios de la digitalización se distribuyan de manera equitativa y se minimicen los riesgos asociados.

2.1.20. Protección de datos

La protección de datos “se refiere a estrategias y procesos de seguridad que ayudan a proteger datos confidenciales frente a corrupción, vulneración y pérdida. Las amenazas a datos confidenciales incluyen incidentes de vulneración y pérdida de datos.” (Microsoft, s.f.)

Además de estas estrategias y procesos, la protección de datos también implica la implementación de políticas y normativas que aseguren el manejo adecuado de la información sensible. Esto incluye la encriptación de datos, el control de acceso a la información y la auditoría

regular de los sistemas de seguridad. La finalidad es garantizar que solo las personas autorizadas puedan acceder a los datos y que cualquier intento de acceso no autorizado sea detectado y mitigado de manera oportuna.

Su importancia se debe a la gran cantidad de información personal y confidencial que maneja la Administración Pública. La protección adecuada de estos datos no solo previene el uso indebido de la información, sino que también fortalece la confianza de los ciudadanos en las entidades públicas.

2.1.21. Neutralidad Tecnológica

La neutralidad tecnológica se refiere al principio según el cual los individuos y las organizaciones tienen la libertad de elegir la tecnología más adecuada a sus necesidades sin depender de conocimientos específicos o datos de una tecnología en particular. Este concepto implica que todos los productos y servicios deben estar al alcance de la mayoría de los usuarios, independientemente de la plataforma, el sistema operativo o el dispositivo móvil que utilicen (Viafirma, s.f.). La neutralidad tecnológica busca evitar la dependencia de una única tecnología, promoviendo así la innovación y la competencia en el mercado.

En la Administración Pública, la neutralidad tecnológica es fundamental para garantizar que los servicios gubernamentales sean accesibles para todos los ciudadanos, sin importar las herramientas tecnológicas que utilicen. Por ejemplo, un portal de servicios públicos debe ser compatible con diferentes navegadores y dispositivos, asegurando que cualquier ciudadano pueda acceder a la información y realizar trámites sin restricciones tecnológicas. Además, la neutralidad tecnológica permite que la Administración Pública adopte las soluciones más eficientes y adecuadas a sus necesidades, sin estar limitadas por contratos o dependencias con proveedores específicos.

Las ventajas de la neutralidad tecnológica son numerosas. En primer lugar, fomenta la competencia y la innovación, ya que las empresas tecnológicas deben esforzarse por ofrecer productos y servicios que sean compatibles con una amplia gama de plataformas y dispositivos. Esto, a su vez, beneficia a los usuarios, quienes tienen más opciones y pueden elegir las soluciones que mejor se adapten a sus necesidades. Además, la neutralidad tecnológica reduce los costos y los riesgos asociados con la dependencia de un único proveedor, permitiendo adaptarse rápidamente a los cambios tecnológicos y aprovechar nuevas oportunidades.

Por lo tanto, la neutralidad tecnológica es un principio esencial para el desarrollo de una sociedad digital inclusiva y dinámica. Su implementación en la Administración Pública no solo mejora la accesibilidad y la eficiencia de los servicios gubernamentales, sino que también promueve la innovación y la competencia en el mercado tecnológico. A medida que la tecnología continúa evolucionando, es crucial que las políticas y regulaciones sigan apoyando la neutralidad tecnológica para garantizar que todos los ciudadanos puedan beneficiarse de los avances tecnológicos de manera equitativa y sin restricciones.

2.1.22. Software

El software se refiere a un conjunto de instrucciones, datos o programas que permiten a una computadora realizar tareas específicas. A diferencia del hardware, que son los componentes físicos de un sistema informático, el software es intangible y se encarga de gestionar y coordinar el funcionamiento del hardware. Según Lenovo, el software puede clasificarse en tres categorías principales: software de sistema, software de aplicación y software de programación (Lenovo, s.f.). El software de sistema incluye sistemas operativos y utilidades que gestionan los recursos del hardware, mientras que el software de aplicación abarca programas que permiten a los usuarios

realizar tareas específicas, como procesadores de texto y hojas de cálculo. Por último, el software de programación proporciona herramientas para que los desarrolladores creen otros programas.

En la Administración Pública, el software juega un papel crucial en la modernización y eficiencia de los servicios gubernamentales. Los sistemas de gestión administrativa, por ejemplo, permiten la automatización de procesos burocráticos, reduciendo el tiempo y los costos asociados con la tramitación de documentos y la gestión de recursos. Además, el software de gestión documental facilita el almacenamiento, organización y recuperación de información, mejorando la transparencia y la rendición de cuentas. Herramientas como los sistemas de información geográfica y los sistemas de gestión de bases de datos también son esenciales para la planificación y toma de decisiones en el sector público.

La diferencia entre software y hardware es fundamental para comprender el funcionamiento de los sistemas informáticos. Mientras que el hardware se refiere a los componentes físicos que componen una computadora, como el procesador, la memoria RAM y el disco duro, el software es el conjunto de instrucciones que le indican al hardware cómo operar. Sin el software, el hardware sería inútil, ya que no tendría la capacidad de realizar ninguna tarea. Por otro lado, el software depende del hardware para ejecutarse, ya que necesita los recursos físicos para funcionar. Esta interdependencia es lo que permite que los sistemas informáticos sean tan versátiles y poderosos.

En el contexto de la Administración Pública, el software de gestión administrativa es esencial para mejorar la eficiencia y la calidad de los servicios ofrecidos a los ciudadanos. Por ejemplo, los sistemas de gestión de recursos humanos permiten la automatización de procesos como la contratación, la gestión de nóminas y la evaluación del desempeño, lo que reduce la carga administrativa y mejora la precisión de los datos. Asimismo, los sistemas de gestión financiera

ayudan a las instituciones públicas a llevar un control riguroso de sus presupuestos y gastos, asegurando una administración transparente y responsable de los recursos públicos.

En conclusión, el software es una herramienta indispensable en la era digital, tanto en el ámbito privado como en el público. Su capacidad para automatizar procesos, gestionar información y mejorar la eficiencia operativa lo convierte en un componente esencial de cualquier sistema informático. En la Administración Pública, el uso adecuado del software puede transformar la manera en que los gobiernos interactúan con los ciudadanos y gestionan sus recursos, promoviendo una gestión más transparente, eficiente y centrada en el ciudadano. A medida que la tecnología continúa avanzando, es crucial que las instituciones públicas adopten soluciones de software que les permitan adaptarse a las demandas cambiantes de la sociedad y ofrecer servicios de alta calidad.

2.1.23. Web

La web "viene a ser un sistema de distribución de información basado en hipertexto o hipermedios enlazados y accesibles a través de Internet." (Eustat, s.f.) también conocida como la World Wide Web, es una plataforma esencial en la era digital que permite la distribución y el acceso a información a través de Internet. Su importancia radica en la capacidad de conectar a personas y organizaciones de todo el mundo, facilitando la comunicación, el intercambio de conocimientos y la colaboración. La web ha transformado la manera en que interactuamos, trabajamos y aprendemos, convirtiéndose en una herramienta indispensable en la vida cotidiana.

La administración pública ha aprovechado la web para acercarse a los ciudadanos de manera más eficiente y transparente. A través de portales gubernamentales, las instituciones públicas pueden ofrecer servicios en línea, como la solicitud de documentos, el pago de impuestos y la consulta de información relevante. Esto no solo mejora la accesibilidad y la comodidad para

los ciudadanos, sino que también promueve la transparencia y la participación ciudadana en los procesos gubernamentales. Por tanto, la web ha revolucionado la forma en que las administraciones públicas interactúan con la sociedad, facilitando un gobierno más abierto y accesible para todos.

2.2.El Acto Administrativo desde la digitalización

Una vez definido el marco conceptual, se puede hablar del Acto Administrativo, el cual señala el jurista Jinesta Lobo con que "no existe una definición jurídico-positiva preestablecida de acto administrativo, sino un conjunto de normas jurídicas que rigen su formación, ejecución, patología y extinción y que-constituyen su régimen jurídico" (2009. p.285), por lo cual, se logra interpretar que el acto administrativo se transforma según los actos formales o materiales que el estatuto jurídico permite realizar. Esto quiere decir que, conforme se constituyan instrumentos normativos dentro del marco de la Administración Pública; el acto puede llegar a tener un mayor alcance y se puede manifestar mediante "una declaración unilateral de voluntad, conocimiento o juicio efectuada en el ejercicio de la función administrativa, que produce efectos jurídicos concretos o generales, de alcance normativo o no, en forma directa o inmediata." (p. 289).

No obstante, el acto administrativo no sólo equivale a una acción o hecho generado por la Administración Pública por su cuenta, ya que implica de su validez conforme al marco del Principio de Legalidad que lo rige. De lo contrario, se declararía la nulidad según los artículos 158 al 179 de la Ley General de Administración Pública, en el cual se divide en dos tipos relativa y absoluta, "según la gravedad de la violación cometida" (Artículo 165, Ley General de la Administración Pública). Debido a que la primera produce saneamiento, al no ausentar o afectar los elementos constitutivos del acto administrativo, a diferencia de la segunda, que impide que

pueda realizarse. Con base a lo anterior, se llega a la eficacia, la cual es la que genera los efectos jurídicos producidos del acto administrativo (pp.402-406).

Asimismo, es importante destacar que la forma más tradicional de ejemplificar el acto administrativo es mediante lo material y escrito, debido a la formalidad que la misma implica y que brinda seguridad jurídica. No obstante, esta no es la única forma posible, ya que, como se mencionó anteriormente, el acto administrativo puede manifestarse en el ejercicio de la función de la Administración Pública, cuya amplitud permite que dicho acto no se limite a un único medio de expresión. Es a partir de este concepto donde la digitalización logra tomar un rol importante en la gestión administrativa, ya que estos no deben ser distintos a lo físico, ya que como señala Agustín Gordillo (2016) en el capítulo VII sobre "Los Administrativos como Instrumentos públicos":

> El hecho de tener soporte no papel no les quita el carácter de actos administrativos, ni obsta a la presunción de legitimidad que les es propia. Así como una luz roja es suficiente para transmitir al conductor de un vehículo la prohibición de avanzar, así también un haz de luz o un holograma puede transmitir otro tipo de mensaje, como también lo puede hacer cualquier soporte físico capaz de contener la información digitalizada de que se trate, en tanto sea comprensible por las personas a las cuales va dirigida.

De la misma forma, esto se logra ver inmerso actualmente en el uso de firmas de documentos digitales donde en la "Ley de Certificados, Firmas Digitales y Documentos Electrónicos (N°8454)" en su artículo tercero expone el reconocimiento de la equivalencia funcional:

> Cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático, se tendrá por jurídicamente equivalente a los documentos que se otorguen, residan o transmitan por medios físicos.

> En cualquier norma del ordenamiento jurídico en la que se haga referencia a un documento o comunicación, se entenderán de igual manera tanto los electrónicos como los físicos. No obstante, el empleo del soporte electrónico para un documento determinado no dispensa, en ningún caso, el cumplimiento de los requisitos y las formalidades que la ley exija para cada acto o negocio jurídico en particular.

Por lo cual, se resalta que la esencia del acto administrativo no radica en el medio material, sino en el contenido que esta posee y su capacidad de producir efectos jurídicos. Ya que como señala Ortiz citado por Gordillo (2016):

> El acto administrativo escrito es plena prueba de su autenticidad en cuanto a fecha, firmas, otorgamiento, pero no de su contenido, ni de los hechos afirmados en su texto por los funcionarios, incluso si son relatados como de su directa visión (p.6).

Lo que da a entender que la instrumentalización mediante el papel únicamente certifica el acto, más no su motivo ni validez (Gordillo, 2016 pp. 5-6). En consecuencia, mientras el instrumento que emite el mensaje sea claro, accesible y cumpla con los elementos constitutivos que exige por el ordenamiento jurídico, puede manifestarse a través de nuevas tecnologías, sin perder su validez.

En este sentido, en el contexto de la transformación digital de la Administración Pública, los elementos constitutivos no desaparecen, sino que se adaptan a nuevas fuerzas de expresión sin perder su legitimidad. Dichos elementos, se logran dividir según Jinesta Lobo en formales y materiales donde estos últimos se logran dividir en subjetivos y objetivos.

En primer lugar, como elemento material subjetivo se encuentra la competencia, la cual Jinesta Lobo citando a Arranz define la competencia como “La aptitud legal para que con unos medios y unas formas predeterminadas realicen sus fines los órganos públicos”, y conforme a lo

estipulado en el primer párrafo del artículo 66 de la Ley General de Administración Pública “Las potestades de imperio y su ejercicio, y los deberes públicos y su cumplimiento, serán irrenunciables, intransmisibles e imprescriptibles” y debe ser dictada por un órgano competente según el artículo 129 de este mismo cuerpo normativo, donde se refuerza aún más exigencia jurídica ante la validez del acto (pp. 312-314).

Con base a lo anterior, esto se logra evidenciar en la utilización de herramientas como los sistemas de autenticación, firmas digitales inclusive las plataformas web que las instituciones estatales que aseguran provenir del órgano competente respectivo, enfocado en una competencia personal, siendo un medio para ejercer sus funciones hacia lo interno y a los administrados.

Como segundo elemento material se encuentra la regularidad en la investidura del funcionario, desde un enfoque propio hacia la digitalización, el artículo 111 de la Ley General de Administración Pública, en su inciso segundo:

> A este efecto considéranse [sic] equivalentes los términos "funcionario público", "servidor público", "empleado público", "encargado de servicio público" **y demás similares, y el régimen de sus relaciones será el mismo para todos**, salvo que la naturaleza de la situación indique lo contrario” (subrayado no es original)

En análisis deja un margen de ambigüedad normativa al incorporar la expresión “demás similares”, misma que permite una interpretación extensiva que podría incluir herramientas digitales dotadas de funcionalidades equiparables a las que ejerce un funcionario público. La redacción brindada por el legislador podría dar lugar al reconocimiento de figuras que, sin estar formalmente investidas, actúen de facto en el ejercicio de funciones públicas. Asimismo, el inciso 1 del mismo artículo emplea el término "persona" sin delimitar si se refiere a una persona física, jurídica o incluso virtual, lo cual refuerza la ambivalencia del concepto.

Cabe señalar, además, el artículo 115 menciona acerca de la figura del funcionario de hecho el cual no posee investidura o la misma se encuentre irregular, puede actuar en situaciones de urgencia o cabios ilegítimos de gobierno según las circunstancias que el mismo artículo indica posteriormente en sus incisos.

En coherencia a la digitalización, la figura del funcionario de hecho puede entenderse como un mecanismo de contingencia que permite dar continuidad a la función pública en caso de que el funcionario público de iure, por cualquier fallo, actualización u otro motivo que impida poder ejercer sus funcionarios de hecho actúa con apariencia de legitimidad en situación excepcionales, amparado en la necesidad de preservar la validez y eficacia de los actos administrativos. Esta figura adquiere particular relevancia ante contextos donde los avances tecnológicos y la flexibilización de los medios de actuación generan escenarios no contemplados por la normativa tradicional.

Asimismo, por otro lado, hay autores como Chiriac & Blaj (2019) que mencionan acerca de la necesidad de un "juez electrónico", el cual se dedique en la fiscalización sobre el acto administrativo. El cual consistiría en realizar una primera revisión de la legalidad y autenticidad del acto administrativo en cuestión y del resto de documentos adjuntos, donde se rechazaría la o la solicitud en caso de que exista un incumplimiento de los requisitos mínimos estipulados por la ley y donde hace hincapié a la necesidad de que siga existiendo un ser humano detrás de la tecnología (p.78). De igual manera, se perfila la posibilidad de un control a lo interno de la administración por parte de esta y a lo externo por la vía judicial (p.78-79).

Seguidamente, se encuentra los elementos materiales de legitimación y voluntad. El primero se define como "la titularidad de la potestad de las atribuciones que brinda la competencia" (Jinesta Lobo, 2009. p. 363), en consecuencia, no basta con sólo la implementación de la herramienta o plataforma, sino que la misma debe cumplir con la titularidad brindada por la

institución pública para ejercer válidamente. Por otra parte, la voluntad, el artículo 113 de la Ley General de Administración Pública expresa lo siguiente:

> 1. El servidor público deberá desempeñar sus funciones de modo que satisfagan primordialmente el interés público, el cual será considerado como la expresión de los intereses individuales coincidentes de los administrados.
>
> 2. El interés público prevalecerá sobre el interés de la Administración Pública cuando pueda estar en conflicto.
>
> 3. En la apreciación del interés público se tendrá en cuenta, en primer lugar, los valores de seguridad jurídica y justicia para la comunidad y el individuo, a los que no puede en ningún caso anteponerse la mera conveniencia.

Dicho artículo lo que implica, es la importancia de que el acto administrativo conforme a lo que estipula el ordenamiento, no competa ser una acción antojadiza o personal del funcionario público ni la Administración Pública, sino que la voluntad sea según el interés público. Mismo que se manifiesta mediante la firma de documentos vía digital, notificación en correos electrónicos, acceso a expedientes digitales de distintas instituciones públicas, entre otros. No obstante, además de lo anterior, se pretende que fortalezca aún más la certeza jurídica y reduzcan la voluntad subjetiva y consigo la posibilidad de la existencia de un vicio, por medio de plataformas automatizadas que legitimen el acto. Donde se registre el ingreso con hora, usuario y contenido, autenticación de firma digital y donde además se demuestre que haya el procedimiento adecuado, plazos y criterios objetivos y proporcionales según el control de legalidad de la Administración Pública.

Dentro de los elementos materiales objetivos, se encuentra el motivo o también llamado “presupuesto de hecho” por Romero Pérez (1982) que lo define como “aquellos presupuestos

factuales que la norma jurídica propone, que le dan fundamento a la emisión y aplicación del acto" (p.97), y donde, además, este autor recalca que dicho elemento debe ser reglado y no discrecional (p.98). Lo anterior, se basa en lo estipulado en el artículo 133 de la Ley General de Administración Pública:

> 1. El motivo deberá ser legítimo y existir tal y como ha sido tomado en cuenta para dictar el acto.
>
> 2. Cuando no esté regulado deberá ser proporcionado al contenido y cuando esté regulado en forma imprecisa deberá ser razonablemente conforme con los conceptos indeterminados empleados por el ordenamiento.

Relacionado a lo anterior, es importante destacar que "el motivo es el antecedente inmediato del acto administrativo, que crea la necesidad pública o particular, y lo hace posible o necesario" (Jinesta Lobo, 2009. p. 371), a lo cual se debe su relevancia. Este se puede manifestar de distintas maneras, ya sea de mera constatación o apreciación.

El artículo 132 de la Ley General señala que, al igual que el Motivo, el contenido debe ser regulado, pero que también debe ser "lícito, posible, claro y preciso y abarca todas las cuestiones de hecho y derecho surgidas del motivo, aunque no hayan sido debatidas por las partes interesadas" (Romero Pérez, s.f, p. 133-134), y a su vez Jinesta recalca que ambos están coordinados "por lo que a un motivo determinado corresponde, normalmente, un contenido específico y viceversa".

Cómo último de los elementos materiales, se encuentra el fin, mismo que "se trata del resultado metajurídico y objetivo último que persigue el acto administrativo en relación con el motivo" (Jinesta Lobo, 2009. p 378), esto quiere decir, que el fin es el último paso para conseguir el acto administrativo. Como se mencionó anteriormente, el acto administrativo debe velar por el interés público, como prioridad, por lo que no depende de la voluntad o lo que desee determinar

el funcionario público, ya que para la validez “no se requiere que haya coincidencia entre el fin objetivo del acto indicado por la ley y el fin subjetivo intentado por el funcionario” (p. 378).

En relación con lo anterior, el fin del acto administrativo debe fundamentarse conforme según la ley, de lo contrario, mediante un juez, según estipula el artículo 131 en su inciso segundo; donde el uso de herramientas digitales no generaría una afectación a la estructura jurídica que lo compone, sino que mejoraría su trazabilidad, transparencia y eficacia.

Enfocándose en estos tres últimos elementos mencionados: motivo, contenido y fin del acto administrativo. En el contexto de la digitalización, en primer lugar, se fortalecería la objetividad que busca el fin, ya que esta sería independiente a la intención subjetiva del funcionario, lo que limitaría la discrecionalidad indebida. Además de ello, se facilitaría el control jurídico, debido a que el motivo y contenido del acto quedarían mejor plasmados en los sistemas digitales. Permitiendo de dicha forma una mejor verificación de los vicios y excesos de poder que vulneran la validez del acto administrativo.

Por otro lado, están los elementos formales, que presentan la forma en la que se externaliza el acto administrativo, siendo el primero de ellos la Forma de Expresión o Instrumentación. Según el artículo 134 de la Ley General de Administración Pública, el principio general es que el acto administrativo, salvo en caso contrario, debe constar por escrito. No obstante, también se admite que sea mediante expresión verbal u oral, en el caso de una advertencia o llamada de atención; mediante signos o símbolos, donde se podría ejemplificar mediante el uso de señalizaciones que pueden expresar la voluntad o decisión; o expresión tácita, implícita y presunta.

El siguiente elemento formal es la motivación, el cual no se debe confundir con el elemento material del motivo. A pesar de lo anterior, la Sala Primera de la Corte en el voto N.º 01266 – 2012 señala que

> existe una intrínseca relación entre motivación y motivo (elemento material objetivo), toda vez que la primera debe permitir el conocimiento del segundo, pero ello en la medida en que resulta esencial para la comprensión y revisión del contenido dispuesto en el acto, y que a la postre define su efecto.

De la misma forma, este mismo voto, afirma basándose en el numeral 136 de la Ley General donde que la motivación "puede ser "sucinta" e incluso "podrá consistir en la referencia explícita o inequívoca a los motivos de la petición del administrado, o bien a propuestas, dictámenes o resoluciones previas". Claro está, también se dispone en la norma de comentario que, en este último supuesto, estas deben ser comunicadas; ello con la finalidad de permitir el conocimiento y la apreciación de los sustentos, fácticos y jurídicos, sobre los que se basa la decisión adoptada".

El último elemento para considerar es el procedimiento. De acuerdo con el artículo 214 de la Ley General de Administración Pública, se tiene como propósito "asegurar el mejor cumplimiento posible de los fines de la Administración; con respeto para los derechos subjetivos e intereses legítimos del administrado, de acuerdo con el ordenamiento jurídico y a su vez "la verificación de la verdad real de los hechos que sirven de motivo al acto final". Enfocándose propiamente en los elementos formales del acto administrativo, las herramientas digitales más recientes que se encuentran inmersas en la Administración Pública no solo alargan su vigencia, sino que, involucran una transformación integra en su garantía y forma de expresión.

Lo anterior, se puede ejemplificar mediante las plataformas como las bases de datos, y en pequeña escala, sistemas automatizados donde se evidencia la validez en documentación y comunicación de la misma forma que lo han conseguido las herramientas físicas, e inclusive, desde un medio más expedita, accesible e integral entre las instituciones estatales como hacia los

administrados. Permitiendo, además el control, tanto técnico como normativo con la finalidad de reducir el sesgo subjetivo del funcionario público o de la misma Administración Pública sobre el interés superior. Asimismo, el procedimiento administrativo que se encuentra enclavado dentro del acto, se ha visto en los últimos años optimizado mediante el expediente digital y las audiencias virtuales, conforme a la Circular N° 137-2020 "Protocolo para la realización de audiencias orales en modalidad virtual total o parcial mediante la utilización de herramientas tecnológica, en Materia Contencioso-Administrativa y Civil de Hacienda Poder Judicial de Costa Rica", donde tiene como que se desarrollen herramientas que sean "robustas y seguras para tramitar los expedientes electrónicos de forma digital, con acceso remoto para las partes, incorporando sistemas de videollamadas para interconectar a personas a las diligencias judiciales sin la necesidad de su presencia física en los despachos judiciales".

Por consiguiente, no solo promueve la celeridad, sino que garantiza el respeto al debido proceso por medio de registros electrónicos accesibles, plazos cumplidos y notificaciones inmediatas, minimizando la discrecionalidad e incrementando la transparencia. Así, la digitalización no sustituye estos elementos, sino que redefine su aplicación conforme a los principios de legalidad y eficiencia administrativa.

En síntesis, el acto administrativo, lejos de ser una figura estática, se presenta como una manifestación dinámica de la voluntad pública, cuya validez y eficacia dependen tanto de su conformidad con los elementos materiales y formales establecidos por el ordenamiento jurídico, como de su adaptación a los nuevos medios tecnológicos. La digitalización no sustituye la estructura jurídica del acto, sino que fortalece su trazabilidad, legitimidad y control, asegurando que el interés público prime sobre cualquier intención particular. En este contexto, el autor José Gustavo Corvalán (2017) afirma que "no se trata sólo de adaptar los procedimientos clásicos a la

tecnología, como si se tratara de sustituir una máquina de escribir por un ordenador básico en las oficinas estatales", ya que "la era digital transforma las interacciones entre Administración y ciudadanía, tornando obsoletos muchos principios y reglas justificados en un sistema sustentado en el papel y las imprentas" (p. 52) Por tanto, la Administración Pública no solo enfrenta una actualización tecnológica, sino una transformación profunda de su estructura y funcionamiento, en relación con las revoluciones industriales pasadas, como se mencionó anteriormente lo cual exige una reinvención sustantiva del Derecho Administrativo en clave digital.

2.3.Gestión Administrativa Digital

Para efectos de esta investigación, se debe definir en primer lugar el término de Gestión, el cual proviene del verbo gestionar que se define como: "ocuparse de la administración, organización, y funcionamiento de una empresa, actividad económica u organismo" (rae, s.f.). Como se expone, este concepto general está encasillado principalmente a instituciones de carácter privado, no obstante, Tullocks Abarca, lo enfoca propiamente hacia la gestión pública de la siguiente manera:

> se refiere al conjunto de actividades, procesos y decisiones llevadas a cabo por las autoridades o funcionarios públicos encargados de planificar, organizar, dirigir y controlar los recursos y servicios que provee el Estado en beneficio de la sociedad. Este campo abarca una amplia gama de funciones, como la formulación de políticas públicas, la administración de presupuestos, la prestación de servicios públicos, la regulación de actividades económicas, entre otros. (2024, p. 3)

Este autor, Tullocks Abarca (2024), también señala la deficiencia y los retos en la que se encuentra la gestión pública como la dificultad de eficiencia, ausencia de calidad en las tareas realizadas y

hasta falta de transparencia; mismas problemáticas que la digitalización tiene como propósito reducir.

Es importante indicar que un concepto propio de Gestión Administrativa Digital no se ha desarrollado en la doctrina, sin embargo, se puede inferir basado en las definiciones que brinda Transformación Digital", "Gobierno Digital", "Administración Electrónica" y "Actuación Administrativa Automatizada".

Con respecto a Transformación Digital, debe ser vista como una necesidad estratégica no como una opción, a lo cual Aliaga Pizarro (2022) lo visualiza como "una oportunidad de mejorar la productividad y el bienestar" no sólo para los servicios públicos sino para el desarrollo económico e integral de un Estado. Asimismo, Romero Diaz hace hincapié de que no debe tratarse únicamente como una obligación constitucional, sino que además debe ser visto como un deber ético debido a los avances tecnológicos y los beneficios que brindan.

En Gobierno Digital, su concepto se enfoca más en el uso intensivo de las Tecnologías de la Información y la Comunicación (TICs), y según la OEA (2006 p. 403) citado por Cruz Romero (2017), se busca para "agilizar los trámites que realizan los ciudadanos, coadyuvar a transparentar la función pública, elevar la calidad de los servicios gubernamentales y, en su caso, detectar con oportunidad prácticas de corrupción al interior de las instituciones públicas".

Conforme estas definiciones, se puede definir a la Gestión Administrativa como toda acción o proceso que ocurre desde el momento en que se brinda un servicio al administrado o se genera una dentro de la propia Administración Pública a raíz del acto administrativo. El termino de "Digital", se empieza a tomar en cuenta en la transformación de los procesos manuales o del papel al formato digitalizado y posteriormente a la automatización de herramientas. Basado en este concepto es importante señalar que el artículo 140 inciso 8 de la Constitución establece que es un

deber del Poder Ejecutivo y principalmente por el presidente de la República velar por el buen funcionamiento de los servicios y dependencias administrativas, por lo cual es importante que exista una adecuada gestión administrativa que vele por los principios generales del derecho, así mismo, cabe decir que la digitalización es la herramienta más viable para cumplir de una forma expedita dicho requisito.

Debido a que se prevé que la gestión administrativa digital sea más allá de una tramitación más ágil, velar siempre por la colaboración hacia la función pública y brindar un servicio de calidad. Lo que implica que la Administración Pública, además de ser quien brinda el servicio hacia el administrado, también se ve beneficiado por la digitalización ofreciendo mayor legitimidad en sus actuaciones, eficiencia, estandarización de procesos, transparencia y control mediante la instauración de normativa que le permita ejercer dicha función según lo estipula el Principio de Legalidad.

Es importante resaltar que, en Costa Rica, ante la ausencia de una institución o un órgano que regule o supervise la gestión administrativa digital con competencias o potestades efectivas para regular y supervisar de manera integral la gestión administrativa digital. Por lo cual las instituciones tanto centralizadas como descentralizadas han buscado suplir esta necesidad de forma independiente implementando sus propios métodos digitales, los cuales generan un costo adicional al presupuesto institucional. En razón a esto, se genera una disparidad en la experiencia ciudadanía donde un mismo trámite puede resultar rápido en una institución, pero lento o más engorroso en otra.

Como bien señala el Quirós Orozco (2025) respaldado por el Ministerio de Planificación Nacional y Política Económica, Costa Rica ha demostrado tener la capacidad de creación de institucionales y modernizarlas de forma interna, sin embargo, cuenta con:

> debilidad para evaluar y rediseñar la institucionalidad en aras de optimizar el uso de los recursos y de aumentar la eficiencia, eficacia, pertinencia, calidad, sostenibilidad y productividad de sus actividades y con el propósito de el mejor cumplimiento de los objetivos que persigue el Sistema Nacional de Planificación. (pp.4-5)

Por ejemplo, existen gobiernos locales que cuentan con plataformas digitales para realizar los trámites como el pago de patentes, permisos de construcción e impuestos, mientras que otras municipalidades dependen de los documentos físicos y las solicitudes presenciales. La ausencia de un marco centralizado de la gestión administrativa digital conlleva a un desnivel en la eficiencia de los trámites, donde se requiere de una estrategia consolidada que permita un crecimiento continuo no burocrático y de beneficio mutuo.

De igual manera, la Carta Iberoamericana de Derechos y Principios en Entornos Digitales, aunque posee un carácter meramente declarativo y no vinculante, busca establecer un marco orientador de principios compartidos que los Estados miembros de la Cumbre Iberoamericana puedan considerar en el proceso de creación y reformas en sus legislaciones nacionales y políticas públicas; señala que la transformación digital debe brindar un trámite que no sea discriminatorio para la ciudadanía, de accesibilidad sencilla, interoperable entre instituciones y sobre todo seguro. Además, hace mención sobre el uso de un sistema de autenticación dentro de la Administración Pública, firma digital y el principio de "una sola vez" (pp.22-24).

2.3.1. Gestión administrativa digital como servicio público.

Desde una perspectiva teórica, es fundamental reconocer que las gestiones administrativas digitales no solo representan una modernización tecnológica, sino que también comparten los principios esenciales que históricamente han definido al servicio público: continuidad, regularidad e igualdad. Estos principios, al ser trasladados al entorno digital, adquieren nuevas dimensiones

que refuerzan el vínculo entre el Estado y la ciudadanía en una sociedad cada vez más interconectada.

A lo largo de la historia, el concepto de servicio público ha evolucionado en función de los contextos políticos, sociales y económicos. Esta evolución ha dado lugar a diversas conceptualizaciones, entre las cuales destacan cuatro enfoques principales.

Servicio público como función pública, en este modelo, la Administración Pública ejerce potestades exclusivas e indelegables, derivadas de su poder de *imperium*. Estas funciones son intransmisibles e imprescriptibles, lo que garantiza la soberanía estatal y evita que actores privados asuman competencias que corresponden únicamente al Estado. En el entorno digital, este principio se traduce en la necesidad de que las plataformas tecnológicas utilizadas por el Estado estén bajo su control directo, asegurando la legitimidad y legalidad de las actuaciones administrativas. En observancia a esta visión la Constitución Política establece en el artículo 121 inciso 14 cuales son los usos y bienes de dominio público que no pueden salir de la esfera estatal, a menos que sea por tiempo limitado y por medio de ley o concesión especial.

Servicio público como fomento, aquí, el Estado actúa como promotor de actividades privadas que contribuyen al interés público, mediante incentivos como subsidios, subvenciones o beneficios fiscales. En el ámbito digital, este enfoque se refleja en el impulso estatal a la innovación tecnológica, el desarrollo de software libre, y la colaboración público-privada para mejorar la infraestructura digital y la accesibilidad de los servicios.

Servicio público en sentido estricto, **e**ste modelo implica que el Estado asume directamente la prestación regular, continua y obligatoria de ciertos servicios esenciales, como salud, educación o justicia. En el contexto digital, esto exige que las gestiones administrativas estén disponibles de

forma permanente, accesible y segura, mediante plataformas interoperables que garanticen la eficiencia y la transparencia en la atención al ciudadano.

Servicio público como gestión económica, en este caso, la Administración Pública participa en la prestación de servicios mediante empresas públicas, regidas por el Derecho Privado. En el entorno digital, este enfoque permite la contratación de servicios tecnológicos, como almacenamiento en la nube, ciberseguridad o desarrollo de sistemas, siempre que se respeten los principios de legalidad, protección de datos y neutralidad tecnológica.

En conclusión, el servicio público es un concepto es constante transformación, que se permea de las situaciones sociales, políticas y económicas, que su interpretación puede ser bastante amplia. Por lo tanto, la visión de la digitalización de las gestiones administrativas no debe entenderse como una simple automatización de trámites, además se puede pensar como una transformación estructural del servicio público. Esta transformación implica repensar y fortalecer los principios jurídicos que lo sustentan, adaptarlos al entorno digital y garantizar que las tecnologías utilizadas respeten los derechos fundamentales de los ciudadanos, especialmente en lo relativo a la protección de datos, la accesibilidad universal y la transparencia institucional. Por lo tanto, se debe continuar con una compilación de la normativa costarricense.

CAPÍTULO III- MARCO NORMATIVO

3. Normativa costarricense vigente aplicable a la digitalización.

La transformación digital en la Administración Pública costarricense ha generado una creciente necesidad de contar con un marco jurídico que regule adecuadamente el uso de tecnologías en los procedimientos administrativos. Esta evolución no solo responde a una exigencia técnica, sino también a una demanda social por servicios más eficientes, accesibles y transparentes. En este contexto, el Derecho Administrativo costarricense se enfrenta al reto de adaptarse a nuevas dinámicas digitales sin perder de vista los principios fundamentales que rigen la función pública, como la legalidad, la proporcionalidad y la protección de los derechos de los administrados.

Para delinear el marco jurídico costarricense que aplica al Derecho Administrativo Digital, es indispensable realizar un análisis exhaustivo de las leyes, reglamentos, decretos ejecutivos y políticas públicas que han sido promulgadas con el objetivo de habilitar, fomentar o regular el uso de herramientas tecnológicas en el sector público. Este análisis permite identificar tanto los avances significativos como los vacíos normativos que aún persisten, especialmente en áreas sensibles como la protección de datos personales, la ciberseguridad, la interoperabilidad entre instituciones y la accesibilidad digital para todos los ciudadanos.

Asimismo, es importante considerar que la normativa vigente no siempre ha sido diseñada específicamente para el entorno digital, lo que ha generado desafíos en su aplicación práctica. Muchas disposiciones legales han sido adaptadas o interpretadas para responder a las nuevas realidades tecnológicas, mientras que otras requieren reformas profundas para garantizar su eficacia en el contexto actual. Por ello, este apartado busca ofrecer una visión integral de la

situación normativa del país en materia de digitalización, destacando los instrumentos legales más relevantes y evaluando su impacto en la gestión administrativa pública.

3.1. Fuentes del derecho administrativo

El estudio de las fuentes del derecho administrativo resulta primordial en el entendimiento de la estructura normativa que impera en las actuaciones de la Administración Pública. Ante la transformación digital que sufre la sociedad, estas fuentes mantienen su vigencia, pero también experimentan una evolución importante. Este capítulo pretende analizar las fuentes tradicionales del Derecho Administrativo y realizar un análisis reflexivo teórico examinando el impacto o ausencia de este, que tiene la digitalización. Esto con el fin de desplegar una visión integrada entre las bases tradicionales y, los desafíos y oportunidades del entorno digital.

3.1.1. Fuentes escritas

En el Derecho Administrativo costarricense, las fuentes escritas son aquellas que jerárquicamente se encuentran establecidas en el artículo 6 de la Ley General de Administración Pública, que establece lo siguiente:

> 1. La jerarquía de las fuentes del ordenamiento jurídico administrativo se sujetará al siguiente orden:
>
> a) La Constitución Política;
>
> b) Los tratados internacionales y las normas de la Comunidad Centroamericana;
>
> c) Las leyes y los demás actos con valor de ley;
>
> d) Los decretos del Poder Ejecutivo que reglamentan las leyes, los de los otros Supremos Poderes en la materia de su competencia;

e) Los demás reglamentos del Poder Ejecutivo, los estatutos y los reglamentos de los entes descentralizados; y

f) Las demás normas subordinadas a los reglamentos, centrales y descentralizadas.

2. Los reglamentos autónomos del Poder Ejecutivo y los de los entes descentralizados están subordinados entre sí dentro de sus respectivos campos de vigencia.

3. En lo no dispuesto expresamente, los reglamentos estarán sujetos a las reglas y principios que regulan los actos administrativos.

Por lo tanto, a nivel del presente este trabajo de investigación, se logran establecer cuáles son las fuentes escritas aplicables al Derecho Administrativo y a la jerarquización de la cual esta se compone, pero que además están enfocadas específicamente en temas relacionados a la digitalización.

3.1.2. Fuentes no escritas

Las fuentes no escritas, como lo son la costumbre, los principios generales del Derecho y la jurisprudencia desempeñan un rol esencial en la dilucidación de criterios jurídicos ante la insuficiencia o la ambigüedad normativa. Al hablar de la digitalización, estas fuentes alcanzan una importancia remozada al tener que enfrentarse a fenómenos que no han sido regulados formalmente por las fuentes escritas. La exploración de estas fuentes y su adaptación al entorno digital resulta importante dada su fuerza vinculante y papel interpretativo ante la falta de normas; además de poseer un rol importante en la misma creación de normas escritas.

En relación con el objeto de estudio solo serán abarcados los principios generales del Derecho, excluyendo a la costumbre y parcialmente a la jurisprudencia debido a su naturaleza más práctica, y donde está ultima será utilizada únicamente para fines explicativos y de fundamentación

en relación con la Sala Constitucional, en cambio, los principios generales del derecho deben verse como menciona Moderne (2025) parafraseando a Pérez Luño:

> i) los principios generales del derecho como "meta normas" (*principia cognoscendi)*, cuya función está ligada al conocimiento del derecho positivo, el que ellos aclaran e informan proporcionando a los usuarios e intérpretes del derecho los elementos lógicos o técnico-formales susceptibles de contribuir a la comprensión y, por eso mismo, a la aplicación y a la evolución del derecho positivo; ii) los principios generales del derecho como normas (*principia essendi*), que forman parte de las reglas del derecho y deben ser ontológicamente conciliados con los otros enunciados normativos (cuya formulación puede ser expresa o tácita), y iii) los principios generales del derecho como conceptos con dimensión axiológica (*prima principia*), postulados éticos portadores de los valores básicos que inspiran el orden jurídico en su conjunto (la justicia, el bien común o interés general, la seguridad jurídica, las buenas costumbres, la paz, etc.).

Por tal motivo la importancia de los principios generales y su adaptación al cambio coadyuva a una evolución más ordenada, con herramientas para suplir lagunas en los casos necesarios y que permitan un crecimiento normativo. En la estructura del Derecho Administrativo costarricense existen varios principios asociados a las Administración Pública, para efectos de este apartado serán abarcados cuatro; el principio de legalidad, el de razonabilidad o proporcionalidad, el de necesidad y el de protección de la confianza legítima.

3.1.2.1. Principio de legalidad.

Jinesta Lobo (2001) lo llama como "el principio general del Derecho Administrativo de más rancio abolengo y de invocación más usual." (p.174). Este principio se encuentra positivizado en el artículo 11 de la Constitución Política

> Los funcionarios públicos son simples depositarios de la autoridad. Están obligados a cumplir los deberes que la ley les impone y no pueden arrogarse facultades no concedidas en ella. Deben prestar juramento de observar y cumplir esta Constitución y las leyes. La acción para exigirles la responsabilidad penal por sus actos es pública. La Administración Pública en sentido amplio, estará sometida a un procedimiento de evaluación de resultados y rendición de cuentas, con la consecuente responsabilidad personal para los funcionarios en el cumplimiento de sus deberes. La ley señalará los medios para que este control de resultados y rendición de cuentas opere como un sistema que cubra todas las instituciones públicas.

Por consiguiente, se deben hacer varios análisis de este principio en relación con la digitalización; primeramente, mencionar que según Jinesta Lobo (2001) "toda actuación o conducta de la administración pública (actos administrativos, actuaciones materiales y servicios públicos) deben estar autorizados por el ordenamiento jurídico de forma expresa o razonablemente implícita." (pp. 174-175) y por esta razón es que este principio siempre es antepuesto al artículo 28 de la Constitución Política que norma el principio base del Derecho Privado de autonomía de la voluntad. Por lo tanto, en Derecho Público solo está permitido lo que la ley indique y en Derecho Privado solo se encuentran prohibidas las actuaciones que estime la ley; además se deben mencionar dos figuras doctrinales que permiten relevar este principio de su relevancia determinante, la discrecionalidad administrativa y los estados de necesidad y urgencia.

En los casos donde los entornos digitales predominan, este principio en sí adquiere importancia en varios sentidos, y la falta de una norma escrita que lo delimite puede causar lesiones a derechos de los administrados. Sí el principio de legalidad provee una cierta rigidez a las funciones y actuaciones administrativas entendiendo que "los entes y órganos públicos únicamente

pueden realizar lo que el ordenamiento jurídico les permite y, consecuentemente, no pueden hacer lo que no les permite." (Jinesta Lobo, 2001, p. 175) pero en materia digital la Administración Pública cuando debe por necesidad incorporar actuaciones o funciones digitales, y no existe norma escrita que las regule entonces cada institución, órgano, empresa estatal, ministerios, municipalidades, juntas, entre otras; deben aplicar el principio de discrecionalidad administrativa para poder incorporar la digitalización en sus respectivos ámbitos. Por ende, pueden surgir problemáticas de diferentes categorías, interoperabilidad, privacidad, manejo de información, acceso a funciones de dispositivos móviles, solo en mención de los muchos de los que pueden brotar.

A pesar de que se han dado intentos de regulación en ámbitos digitales, las existentes no son de Derecho Público *per se,* a pesar de que puedan ser utilizadas para regular ámbitos de la Administración Pública, no se ha legislado con normativa que logre respetar no solo el principio de legalidad, si no temas sensibles como lo son los metadatos, las *cookies,* permisos otorgados, y demás. En consecuencia, las aplicaciones y sitios web pertenecientes a la Administración Pública al estar por la libre y con la presión de una digitalización forzada, delega a la discrecionalidad administrativa la decisión de la información que se recolecta, y si esta se almacena en una base de datos, pero aún más importante quién tiene autorización dentro su investidura para visualizar, acceder, gestionar y hasta modificar dicha información.

No obstante, estos datos que se recolectan de manera automática por medios digitales pueden llegar a reforzar el principio de legalidad desde la óptica de evaluación de resultados y la rendición de cuentas, ya que su tratamiento y estudio debido puede llegar a detectar uso, problemas, accesos, modificaciones y otros, que permitan gestionar los actos administrativos con información invaluable para la seguridad, el cumplimiento normativo y la gestión de permisos.

En resumen, no existe un ordenamiento jurídico que de una forma expresa o razonablemente implícita regule y autorice las actuaciones y la conducta de la Administración Pública en los entornos digitales, arrogando al principio de la discrecionalidad administrativa la atribución de determinar las capacidades de sus procesos digitales, en contraposición al principio de legalidad que puede generar abusos por parte de la Administración Pública pero también en desaprovechamiento para de estas herramientas para poder generar mejoras en ámbitos variopintos dentro de las instituciones convergiendo en la mejora de los servicios brindados a los administrados.

3.1.2.2. Principio de razonabilidad o proporcionalidad

El principio de razonabilidad o proporcionalidad es un principio de primer orden que no solo se ata al principio de legalidad si no que funciona como límite al principio de discrecionalidad administrativa.

Este principio ha sido desarrollado a nivel costarricense de manera jurisprudencial, por ejemplo, el voto 8858-1998 de la Sala Constitucional, la misma indica tres criterios esenciales: necesidad, idoneidad y proporcionalidad. Por lo que cualquier acto de la Administración Pública debería ser necesario para que se cumpla un fin, en otras palabras, si este acto no se realiza puede existir una lesión a algún interés público. Pero, además el medio escogido para realizarlo debe ser el idóneo con el propósito de la actuación que se pretende realizar cumpla con la finalidad de satisfacer la necesidad que se intenta suplir. Como corolario de este principio debe ser proporcional, para que en caso de que esta actuación provoque una lesión a un derecho personal esta sea la menos gravosa posible.

Sumado a lo abordado por la misma Sala en la resolución 00732 – 2001, donde la Sala aborda la doctrina estadounidense, y el origen del principio de razonabilidad desde el ángulo

procesal, estableciendo que según sea el caso debe realizarse un juicio de razonabilidad, primeramente, determinando la "razonabilidad técnica" que básicamente es realizar el ejercicio supra mencionado de necesidad, idoneidad y proporcionalidad. Aunando la determinación de la "razonabilidad jurídica" que se puede establecer en si existe razonabilidad ponderativa, de igualdad y en el fin; que se puede interpretar como una valoración jurídica ante la existencia de un antecedente que pueda determinar una equivalencia en la actuación, siempre buscando la menos gravosa.

En resumen, al realizar un acto administrativo se debe practicar un análisis jurídico con el fin de determinar cuál debe ser el camino por seguir, si es posible realizar la actuación desde la discrecionalidad administrativa o si debe ser necesario aplicar los principios generales y las fuentes escritas.

Ahora bien, en el caso de las actuaciones digitales, y como se describe en el apartado anterior, mucho del ámbito digital está por la libre y permite que entre en juego la discrecionalidad administrativa. Por lo que la Administración debe realizar el ejercicio de los tres criterios esenciales; sobre la necesidad, la Administración debe sí o sí mudar casi la totalidad de sus actuaciones al contorno digital, por lo que carece de sentido la discusión sobre la necesidad, más bien, la falta de digitalización infringe este criterio ya que al no ser realizada importantes interese públicos pueden ser contravenidos.

La idoneidad, es el tema que tiene mayor cantidad de aristas a evaluar, actualmente en tema de tecnología, existen gran variedad de sistemas operativos y de dispositivos que inundan el mercado, además de nuevas tecnologías que llegan casi diariamente, a lo que se le debe sumar la Inteligencia Artificial, por lo que el medio a escoger puede ser muy vario y de igual manera cumplirá con la necesidad. Por lo tanto, se puede pensar en otros parámetros a la hora de determinar

la idoneidad de un medio digital, y bajo la misma línea evolutiva del Derecho Público se debe hacer mención tres factores primordiales: ciberseguridad, interoperabilidad y rentabilidad.

Primeramente, la Administración Pública debe garantizar que la idoneidad del medio que use sea cibersegura para el administrado y que este no vea comprometida su gestión e información; la interoperabilidad, los sistemas, aunque no compartan la misma función y puedan variar entre sus funciones estos deben poder intercambiar información y, además deben poder desplegar sus funciones en las terminales de los administrados. El tema de rentabilidad en vista de que los sistemas deben ser rentables a través del tiempo, con la posibilidad que la Administración logré costear mantenimiento, reparación y actualización de esta.

Para finalizar, la proporcionalidad, con este sucede algo parecido al criterio anterior, desde una visión somera de que, si la digitalización es proporcional, no existe ninguna lesividad para el administrado por lo que la respuesta es afirmativa. Empero con un análisis sensato se encuentra que las herramientas digitales poseen la capacidad de extraer datos desde las terminales que utilice el administrado y a través del análisis de *big data* extraer información valiosa, no se debe deducir que esta afirmación es negativa ya que el estudio de estos datos también pueden generar un cambio positivo mediante mejoras en políticas clave, aunque en casos más gravosos se podría extraer información que permita individualizar la información a un administrado lesionando el principio de autodeterminación informativa, de consentimiento informado y el derecho a la intimidad. La proporcionalidad en la digitalización debe ser explorada con razón a cuál información es la necesaria para recopilar y analizar en proporción a que la lesividad a los derechos personales del administrado sea mínima o nula.

3.1. Constitución Política de Costa Rica

La Carta Magna costarricense de 1948, debido a su contexto histórico y temporalidad, no contemplaba originalmente disposiciones relacionadas con la digitalización, ni con el uso de tecnologías de la información en el ámbito estatal o administrativo. Sin embargo, reconociendo la evolución tecnológica y la creciente necesidad de garantizar derechos fundamentales en entornos digitales, en el año 2023 la Asamblea Legislativa aprobó una reforma significativa al artículo 24 de la Constitución Política, que se puede leer de la siguiente manera:

> "ARTÍCULO 24.- Se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones. Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República. Sin embargo, la ley, cuya aprobación y reforma requerirá los votos de dos tercios de los Diputados de la Asamblea Legislativa, fijará en qué casos podrán los Tribunales de Justicia ordenar el secuestro, registro o examen de los documentos privados, cuando sea absolutamente indispensable
>
> Toda persona tiene el derecho fundamental al acceso a las telecomunicaciones, y tecnologías de la información y comunicaciones en todo el territorio nacional. El Estado garantizará, protegerá y preservará este derecho." (Constitución Política de Costa Rica, 1948, Art. 24)

A pesar de que, en un contexto histórico donde la digitalización no formaba parte de la realidad social ni jurídica, es posible identificar disposiciones que, por su naturaleza, resultan fundamentales para el desarrollo normativo en entornos digitales. Entre ellas destacan el derecho a la intimidad y el secreto de las comunicaciones, los cuales han sido reconocidos como pilares esenciales en la protección de los derechos fundamentales frente a los desafíos que plantea la digitalización. Estos derechos, ya mencionados en el presente trabajo investigativo, se configuran

como garantías constitucionales que resguardan la esfera privada de los individuos, incluso en el ámbito digital.

La inviolabilidad de las comunicaciones adquiere una relevancia particular en el contexto actual, al extenderse a todo tipo de comunicación, ya sea escrita, oral o de cualquier otra índole. Esta redacción amplia permite interpretar que las comunicaciones digitales como correos electrónicos, mensajes en plataformas digitales, videollamadas y otros medios electrónicos, también se encuentran protegidas bajo el manto constitucional, lo que abre la puerta a una integración más explícita del entorno digital dentro del marco jurídico costarricense.

Además, la reforma constitucional aprobada en el año 2023, que incorporó el derecho fundamental de acceso a las tecnologías de la información y las comunicaciones (TICs), representa un hito trascendental en la evolución del ordenamiento jurídico nacional. Esta adición no solo reconoce el acceso a las TICs como un derecho inherente a todos los habitantes del país, sino que también impone al Estado la obligación de garantizar, proteger y preservar dicho acceso en todo el territorio nacional. En consecuencia, se sientan las bases para que la digitalización no sea vista únicamente como una herramienta técnica o administrativa, sino como un componente esencial del ejercicio de derechos ciudadanos.

Este reconocimiento constitucional implica que, en el futuro, la digitalización deberá consolidarse como una política pública transversal, orientada a fortalecer la inclusión, la eficiencia administrativa y la transparencia institucional. Por consiguiente, obliga a que las instituciones estatales desarrollen mecanismos normativos, técnicos y operativos que aseguren el acceso equitativo a las Tecnologías de la Información y la Comunicación (TICs), especialmente para poblaciones vulnerables o con limitado acceso a recursos tecnológicos.

En síntesis, aunque la Constitución fue concebida en una época previa a la revolución digital, su evolución normativa y la interpretación progresiva de sus principios permiten afirmar que el entorno digital ya forma parte del marco constitucional costarricense. Esto refuerza la necesidad de que el Derecho Administrativo se adapte a esta nueva realidad, garantizando que la digitalización se implemente de manera armónica, legal y respetuosa de los derechos fundamentales.

3.2. Ley General de Administración Pública N°6227

La transformación digital de la Administración Pública costarricense ha generado una reconfiguración profunda de los principios que históricamente han regido el servicio público. En este contexto, el artículo 4 de la Ley General de la Administración Pública adquiere una relevancia renovada.

> Artículo 4º.-La actividad de los entes públicos deberá estar sujeta en su conjunto a los principios fundamentales del servicio público, para asegurar su continuidad, su eficiencia, su adaptación a todo cambio en el régimen legal o en la necesidad social que satisfacen y la igualdad en el trato de los destinatarios, usuarios o beneficiarios. (Ley General de la Administración Pública, N.º 6227, 1978, art. 4).

Esta disposición normativa, aunque promulgada en un contexto anterior a la revolución digital, contiene elementos que se proyectan con fuerza en el entorno tecnológico actual, donde la digitalización no solo representa una herramienta de modernización, sino una exigencia jurídica y social.

El principio de continuidad del servicio público encuentra en la digitalización una vía para su fortalecimiento. La implementación de plataformas digitales, sistemas automatizados y servicios en línea permite que las instituciones estatales mantengan su operatividad incluso en

situaciones de emergencia. La posibilidad de acceder a trámites, información y servicios sin interrupciones temporales ni barreras geográficas responde directamente al mandato legal de garantizar la permanencia del servicio público. No obstante, esta continuidad depende de la existencia de una infraestructura tecnológica robusta, de políticas de ciberseguridad efectivas y de una gestión institucional que priorice la resiliencia digital.

La eficiencia, como principio rector del servicio público, se ve potenciada por la digitalización mediante la automatización de procesos, la reducción de tiempos de respuesta y la optimización de recursos. Herramientas como el Sistema Integrado de Compras Públicas (SICOP), la firma digital y los sistemas interoperables entre instituciones permiten una gestión más ágil, transparente y menos burocrática. Sin embargo, esta eficiencia debe estar respaldada por un marco jurídico sólido que garantice la legalidad de los actos administrativos digitales, evitando arbitrariedades y asegurando la trazabilidad de las decisiones.

La adaptación al cambio legal y social, otro de los principios consagrados en el artículo 4, se manifiesta en la necesidad de que la Administración Pública evolucione conforme a las transformaciones tecnológicas y las nuevas demandas ciudadanas. La digitalización debe ser vista como una respuesta institucional a una sociedad cada vez más interconectada, donde los ciudadanos demandan servicios públicos ágiles, accesibles y centrados en sus necesidades.

Finalmente, el principio de igualdad en el trato adquiere una dimensión crítica en el entorno digital. La implementación de tecnologías debe garantizar la accesibilidad universal, especialmente para personas con discapacidad, adultos mayores, poblaciones rurales y ciudadanos con alfabetización digital limitada.

3.3.Ley General de Telecomunicaciones N°8642

Esta ley regula mayormente lo referente al acceso a las Tecnologías de la Información y la Comunicación (TICs) por parte de los usuarios y el mercado de telecomunicaciones. Pero en los artículos 42 y 43 de esta ley se encuentra la regulación sobre privacidad de las comunicaciones y protección de datos personales concordantes con el artículo 24 de la Constitución Política y además de una regulación sobre los datos de tráfico y localización, así como su tratamiento por parte de los operadores y proveedores.

Sobre el tema de privacidad de las comunicaciones y protección de datos personales, además de lo supra mencionado, obligando a los operadores y proveedores de los servicios a tomar medidas que impidan que las comunicaciones sean "escuchadas, gravadas(sic), almacenadas, intervenidas ni vigiladas por terceros sin su consentimiento(...)" (Ley General de Telecomunicaciones, Artículo 42).

En cuanto al tema de datos de tráfico y localización, la ley lo que establece es que estos deberán eliminarse o hacerse anónimos para su tratamiento. Al tratarse de datos de tráfico que son usados para la facturación solo podrán almacenarse por el tiempo que legalmente se pueda impugnar o exigirse el pago. Respecto a los datos de localización, solo podrán tratarse si se hacen anónimos o si hay consentimiento del abonado o usuario y solo en medida y tiempo para la prestación del servicio.

3.4.Ley de Planificación Nacional N°5525

Esta ley de 1974 a pesar de ser anterior incluso a la Ley General de Administración Pública, por lo que en aporte a la digitalización per se no incorpora absolutamente nada, pero si se encuentra importancia debido a que incorpora al Ministerio de Planificación Nacional y Política Económica

(MIDEPLAN) como el actor encargado en materia de modernización y reforma de la Administración Pública central y descentralizada con excepción de las instituciones que cuenten con autonomía constitucional o libre competencia. Para lograr este cometido se cuenta con la Comisión de Eficiencia Administrativa.

Consecuentemente, también se designa al MIDEPLAN como el ministerio encargado de la coordinación interinstitucional por lo que se puede inferir que debe ser partícipe en la creación de mecanismos digitales que permitan la intercomunicación de los sistemas utilizados por las instituciones.

3.5. Ley Promoción Desarrollo Científico y Tecnológico y Creación del MICYT (Ministerio de Ciencia y Tecnología) Nº7169

Inicialmente, esta ley de 1990 creó el Ministerio de Ciencia y Tecnología (MICYT) con la iniciativa de que el país se enrumbará a una era de ciencia y tecnología, agregando está cartera ministerial al Poder Ejecutivo. En los artículos 20 y 21, se le otorgan las atribuciones como órgano rector de la materia. Esta ley ha sufrido siete reformas a lo largo de los años, aunque para razones del presente trabajo investigativo se debe mencionar la reforma de la Ley N°9046 Traslado del Sector Telecomunicaciones del Ministerio de Ambiente, Energía y Telecomunicaciones al Ministerio de Ciencia y Tecnología de 2012, que conllevó en su momento a que este ministerio absorbiera la competencia del área de telecomunicaciones del país pasando a llamarse Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) como es conocido actualmente y la reforma de la ley N°9971 Ley de Creación de la Promotora Costarricense de Innovación e Investigación de 2021, la cual reformó los artículos 20 y 21 “actualizando” las funciones del MICITT.

A pesar de que ninguna de las leyes anteriores trata sobre digitalización de la Administración Pública o del Derecho Administrativo digital, cabe destacar que el MICITT a través de otras normativas adquiere la competencia por materia de esta área digital al estar ligada a la innovación y tecnología que el legislador busca promover mediante estas normativas.

3.6. Ley de Certificados, Firmas Digitales y Documentos Electrónicos N°8454 y su reglamento

La ley N°8454 es una normativa sencilla, promulgada del 2005, que permite usar una tecnología basada en la infraestructura de llave pública o PKI por sus siglas en inglés y la norma INTE /ISO 21188, permitiendo emitir y comprobar certificados digitales, en este caso de firma digital, con un estándar seguro y que pueden ser utilizados para realizar diferentes tipos de negocios jurídicos donde la firma de una persona sea esencial para la validez del acto, también aclarando que las instituciones deben mantener una manera presencial para realizar cualquier gestión ya que la digitalización por parte del administrado es opcional.

Esta norma define una ruta muy clara designando al Ministerio de Ciencia, Tecnología y Comunicaciones (MICITT) como el ente que maneja a la Dirección de Certificadores de Firma Digital (DCFD) y ante la solicitud de un certificador y con los requerimientos que establezca el Ente Costarricense de Acreditación (ECA, este ente fue creado en 2024 a través de la Ley del Sistema Nacional para la Calidad N°10473) y que basados en la norma INTE-ISO/IEC 17021 busca operar de manera competente, consistente e imparcial. El certificador será la persona jurídica que se encargue de emitir y respaldar los certificados de firma digital además de mantener un repositorio público de los mismos para su verificación y seguridad.

Esta ley aplica cuatro principios, el de regulación mínima y desregulación de trámites, autonomía de la voluntad de los particulares para reglar sus relaciones, el de utilización, con las

limitaciones legales, de reglamentos autónomos por la Administración Pública para desarrollar la organización y el servicio, interno o externo y el de igualdad de tratamiento para las tecnologías de generación, proceso o almacenamiento involucradas. A los cuales se les debe sumar los principios de neutralidad tecnológica y el de interoperabilidad. Además, designa a la Dirección General del Archivo Nacional a través del artículo 6 como el ente encargado de girar las regulaciones sobre lo referente a la gestión y conservación de documentos electrónicos, en relación con la Ley del Sistema Nacional de Archivos Nº7202 de 1990 y su reglamento.

Esta ley permite realizar el registro del solicitante cara a cara, aunque optativamente deja la posibilidad de realizar un registro remoto mientras cumpla con requisitos para evitar suplantación de identidad, y obliga a los certificadores a guardar tantos los documentos del registro como los datos biométricos del suscriptor.

En resumen, esta ley logra crear una plataforma sólida y segura que permite emitir actos jurídicos digitales de diferentes tipos tanto privados como públicos a través de certificadores que se encuentran certificados y fiscalizados por entes públicos, definiendo muchos conceptos que en la actualidad son esenciales en la digitalización y que permitiría partir de una base sólida para digitalizar la Administración Pública, empero a pesar de los 20 años que posee esta ley , su evolución solo se ha enmarcado en el marco de firmas digitales y no se ha aprovechado su solidez para mejorar y agilizar las gestiones administrativas.

3.7.Ley de protección a la persona frente al tratamiento de sus datos personales N° 8968 y su reglamento

Esta ley de orden público que entró en vigor en setiembre de 2011 tiene como objetivo garantizar el derecho a la autodeterminación informativa de cualquier persona dentro del territorio nacional ante el tratamiento manual o automatizado de datos relacionados a su persona, actividades

privadas, bienes y demás que puedan ser recopilados. La importancia de esta ley en relación con el tema de la digitalización yace en que las gestiones administrativas digitales pueden acarrear mucha *big data* que puede ser analizada por la Administración Pública de múltiples maneras, desde su uso para crear políticas de mejor alcance al entender dinámicas sociales, hasta lesivas donde la Administración sobrepase el derecho a la intimidad del administrado ejerciendo control sobre cualquier aspecto de la vida personal.

A pesar de que el contexto histórico y el espíritu de la ley al momento de su promulgación puede ser ambiguo, en un análisis detallado exuda una gran integridad dentro del articulado, incorporando al mundo jurídico nacional importantes definiciones y protecciones a derechos de las personas, además de crear la Agencia de Protección de Datos de los Habitantes (PRODHAB) ente al cual se deben inscribir las bases de datos para supervisión, eso sí, es una norma que no ha sido reformada y que si posee algunos vacíos y desactualizaciones que se deben abordar.

3.7.1. Definiciones, principios y derechos básicos que introduce la ley

La ley N°8968 hace introducción a varias definiciones básicas dentro del lenguaje de protección de datos como lo son base de datos, datos personales, de acceso irrestricto y de acceso restringido, datos sensibles, deber de confidencialidad, responsable de la base de datos, interesado y tratamiento de datos personales.

Con respecto a los datos personales es importante la distinción que realiza la ley de los datos personales de acceso irrestricto de los de acceso restringido, la ley N°8968 (2011) detalla a los primeros como “los contenidos en bases de datos públicas de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados.” y a los segundos como “los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública.”, a estas

definiciones se le debe sumar la distinción que hace la ley sobre datos sensibles como los relativos al fuero íntimo de la persona y enlista la raza, opiniones políticas, religión, condición socioeconómica, información genética o biomédica, vida y orientación sexual. Estas definiciones crean un límite definido entre cuales datos se pueden o no recibir tratamiento de datos, que también es regulado por esta ley taxativamente como "el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a estos"

Continuando con los tres principios que incorpora que serían el principio de autodeterminación informativa, de consentimiento informado y el de calidad de la información.

El primero, de autodeterminación informativa definiendo este como un derecho fundamental y se basa en que el individuo tiene derecho del contenido y tratamiento de sus datos con sus respectivas excepciones. El segundo, de consentimiento informado, este principio obliga de manera expresa, precisa e inequívoca a las personas o sus representantes a ser informados de la existencia, fin, destino, tratamiento y demás pormenores de una base de datos y que se debe dar consentimiento al suministrar la información, eso sí con las excepciones de los datos irrestrictos y los solicitados con fundamento legal; también se advierte que el acopio de datos sin consentimiento o adquiridos de manera ilícita, fraudulenta o desleal queda prohibido. Para finalizar, el principio de calidad de información, el encargado de la base de datos debe asegurarse que la información que se trata es actual, veraz, exacta y adecuada al fin.

Sobre los derechos la ley añade únicamente dos, el derecho al acceso a la información y de rectificación de la información; el primero es el derecho que tiene el interesado en solicitar un informe detallado, redactado de manera entendible con explicación del lenguaje técnico sobre la información que yace en una base de datos y la rectificación es el derecho que posee el interesado

en rectificar, actualizar y eliminar los datos, esto último en base a un carácter incompleto o inexacto de la información o que hayan sido recopilados sin autorización, también este derecho confiere la potestad a los sucesores o herederos de una persona difunta a realizar esta solicitud.

3.7.2. Reglamento

En el reglamento de esta ley, se encuentran de manera más amplia definiciones que también tienden a ligar más el objeto de la ley a la información digital, añade el mecanismo de revocación del consentimiento y provee a la ley del derecho al olvido, este derecho lo que agrega es que la información que pueda afectar al titular no deberá exceder los diez años salvo disposición legal contraria. Además, reglamenta parámetros mínimos de seguridad de datos, y en caso de alguna vulneración el deber de informar al titular. El reglamento también determina los supuestos de inscripción, tratamiento, denuncias, pago de multas y cánones, para todo lo referente a la ley.

3.8. Ley de Creación de la Agencia Nacional de Gobierno Digital N°9943 y su reglamento

Esta ley de Derecho Público promulgada en 2021 pero reglamentada hasta 2024, estableciendo la creación de la Agencia Nacional de Gobierno Digital (ANGD), que tiene como objetivo primordial modernizar a la Administración pública mediante implementación y ejecución de servicios y proyectos digitales estratégicos, en busca de simplificar, agilizar, transparentar el acceso a los servicios públicos, por medio del fomento a la eficiencia gubernamental y la promoción de un clima de negocios competitivo, esto bajo el ojo rector del Ministerios de Ciencia, Tecnología y Telecomunicaciones (MICITT) a la cual estará adscrita la ANGD, aunque esta última tenga independencia operativa.

La importancia de esta ley para el objeto de la presente investigación yace en que reconoce la necesidad de la Administración Pública en digitalizar las gestiones administrativas en busca de mayor transparencia, eficiencia y ahorro. Define de manera precisa el derecho que posee los sujetos físicos y jurídicos a relacionarse por medios digitales con la Administración Pública, incorporando el uso de las Tecnologías de la Información y la Comunicación (TIC) en los procesos de atención ciudadana y procesos internos.

Cabe destacar que esta ley define Gobierno Digital como:

> El uso sistemático de las tecnologías de la información y de la comunicación en las instituciones de la Administración Pública, para mejorar la información y los servicios ofrecidos a los ciudadanos, orientar la eficacia y la eficiencia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la activa participación de los ciudadanos. (Creación de Agencia Nacional de Gobierno Digital, Artículo 3 inciso a)

De la misma forma, la ley hace hincapié en la interoperabilidad de los sistemas, y que estos deben tener la capacidad de compartir datos e información en busca de un Estado más eficiente, transparente y participativo, por lo que designa a la ANGD como el ente ejecutor y administrador de la interoperabilidad a nivel técnico.

Consecuentemente, en el reglamento de la ley se incorpora una definición que es de suma importancia, debería estar más delimitada, pero en sí que sea ya parte de la normativa costarricense presenta un avance dentro del Derecho Público como medio para limitar el poder de imperio de la Administración Pública y esta es la identidad digital, y se define como "(...)una representación digital de la información que se conoce sobre un individuo, un grupo, una entidad o un producto específico." (Reglamento de Creación de Agencia Nacional de Gobierno Digital, Artículo 3 inc. b)

3.9. Ley de Protección al Ciudadano del Exceso de Requisitos y Trámites Administrativos N°8220, y su reglamento

La ley 8220 creada en 2002 y reformada varias veces, siendo la última en 2023 ha sido un intento por agilizar la burocracia de las gestiones administrativas. Sus reformas primordialmente han sido para agregar temas referentes a la digitalización que por el tiempo que está ley se ha encontrado vigente se ha ido desactualizando y por ende han sido necesarias.

En ella se puede encontrar disposiciones interesantes, como, el deber de la Administración Pública en apego a la normativa que dicho trámite debe estar por disposición escrita para poder ser solicitado , publicado en La Gaceta y que, además todos los trámites deben estar indicados en un Catálogo Nacional de Tramites a cargo del Ministerio de Economía, Industria y Comercio (MEIC), que mantendrá soporte del Catálogo pero que es responsabilidad de cada institución actualizar de manera obligatoria la información de sus trámites dentro del mismo. En cada trámite se puede incluir instructivos, manuales, formularios y anexos necesarios para su realización en aras de que exista un principio de publicidad e información.

Continuando con la aplicación del silencio positivo en un trámite mediante plataforma digital, indicando de manera similar al procedimiento análogo, primeramente, que solo es permitido en los trámites que se encuentran estipulados, y que mientras el administrado cumpla con todos los requisitos establecidos y que, una vez vencido el plazo, no es necesario que se realice declaración jurada o trámite en la institución, el administrado puede entender inmediatamente como silencio positivo pero se debe verificar el reglamento de la plataforma.

Además, establece principios para la coordinación institucional e interinstitucional que permita el acceso a bases de datos mutuamente o por defecto a que exista una comunicación entre instituciones que permita la solicitud de información sin intermediación del ciudadano.

Se le debe sumar que, para gestiones administrativas digitales, se debe crear un expediente digital que recabe toda la información de este y su estado actual, este expediente debe ser de acceso para el interesado mediante un código de ingreso para que pueda consultar el estado de dicho expediente electrónico durante las 24 horas del día.

La Ley 8220 representa un esfuerzo significativo por modernizar y agilizar los trámites administrativos en Costa Rica, especialmente mediante la incorporación de herramientas digitales. Sus reformas han buscado adaptarse a los retos de la transformación tecnológica, promoviendo principios como la publicidad, la interoperabilidad institucional y el acceso digital a la información. No obstante, su implementación aún enfrenta desafíos, como la necesidad de una mayor estandarización y supervisión interinstitucional. En este contexto, la ley se perfila como un instrumento clave para consolidar una gestión administrativa más eficiente, transparente y centrada en el ciudadano.

3.10. Decreto Ejecutivo N°44507-MICITT Código Nacional de Tecnologías Digitales

El Código Nacional de Tecnologías Digitales (CNTD) emitido por el MICITT, surge ante la prioridad de la Administración Pública de dotar un marco de transformación digital al Estado y es una pieza fundamental dentro de la Estrategia de Transformación Digital hacia la Costa Rica del Bicentenario 4.0 (ETDCR4) y definiendo su propósito como el de “brindar los criterios técnicos básicos que todo proyecto digital debe contemplar para su desarrollo dentro de las instituciones de la administración pública” (CNTD, p. 6). Además, pretende una estandarización de los servicios digitales que se brindan por parte de la Administración Pública a través de un “Sello de Gobierno Digital”.

El CNTD se desarrolla en seis temas fundamentales

3.10.1. Accesibilidad, Usabilidad y Experiencia de Usuario.

El CNTD mediante este capítulo y respetando la normativa nacional e internacional sobre accesibilidad, establece parámetros mínimos para las plataformas digitales cuenten con acceso universal para gestiones administrativas, esto quiere decir que dichas plataformas pueden ser usadas por cualquier persona independientemente de su condición.

Esto se logra a través de la adopción de los Siete Principios del Diseño Universal que son:

- Uso equitativo.
- Flexibilidad en el uso.
- Uso simple e intuitivo.
- Información perceptible
- Tolerancia al error
- Esfuerzo físico bajo
- Tamaño y espacio para aproximación y uso

Sumado a estos principios las plataformas deben ser medidas por su usabilidad, esto se logra usando cinco componentes: aprendizaje, eficiencia, memorabilidad, errores y satisfacción. Lo anterior basado en estándares internacionales ISO 9241-210 y WCAG 2.1 pero además deben de contar con formatos de comunicación accesible (audio, braille, LESCO, lectura fácil, entre otras).

Con respecto a la accesibilidad y usabilidad, no solo es un tema actual dentro del diseño de proyectos digitales, sino que también se relaciona con el cumplimiento de normativa nacional como lo son las leyes N°7600 y N°8642, y normativa internacional como la Convención Interamericana para la eliminación de todas las formas de discriminación contra las personas con discapacidad.

En cuanto a experiencia del usuario, el CNTD hace énfasis que, para poder lograr un desarrollo más acelerado, los proyectos de Gobierno Digital deben contar con 16 estándares digitales, para objeto del presente trabajo investigativo se deben mencionar los equipos multidisciplinarios, código abierto y los que refieren a pruebas, monitoreo e investigación del proyecto. Empezando con los equipos multidisciplinarios, el CNTD solo hace referencias a disciplinas del área tecnológica dejando por fuera la disciplina legal, situación que ya ha sido abarcada y que puede generar que el proyecto lesione algún derecho del administrado por desconocimiento. Otro punto sería el código abierto, este indica que todos los proyectos de la Administración Pública deben ser de código abierto, para que este pueda ser reutilizado por otras instituciones y que se encuentre en un repositorio; esto significa que el propietario de ese código debe ser el Estado, solo que no se define quién tendrá acceso al repositorio. Para finalizar, el tema de pruebas, monitoreo e investigación es un tema más delicado ya que los proyectos pueden recolectar metadatos, que sí, sirven para mejorar las plataformas y corregir errores, pero no se define ningún método de protección ante el tratamiento de estos datos o su individualización.

3.10.2. Identificación y Autenticación Ciudadana.

El CNTD establece que se debe “cumplir con la eficaz identificación y autenticación de los ciudadanos a la hora de utilizar servicios y sistemas en línea, lo cual, en última instancia, brindará seguridad y confianza plena" (p. 55). Aunado a la incorporación de dos principios claves, el de “solo una vez”, las personas tanto físicas como jurídicas solo suministran la información estándar por una única vez, y el de “limitación de la finalidad” refiere a que los datos que se suministran solo pueden ser tratados con la finalidad explícitamente indicada.

Con el objeto de realizar una verificación de la persona usuaria se remite a los mecanismos oficiales de autentificación como lo son la cédula o DIMEX según corresponda, los datos

biométricos o la firma digital, y además se debe incluir el doble factor de autentificación para realizar una identificación inequívoca. Para lograr este cometido se pretende utilizar las bases de datos biométricos que poseen el Tribunal Supremo de Elecciones (TSE) y de la Dirección General de Migración y Extranjería (DGME); estos datos biométricos deben cumplir con normativa internacional, en fotografía cumplir con los requisitos ICAO (International Civil Aviation Organization) y para huellas digitales formato de intercambio ANSI/NIST-CSL 1-1993 con cifrado y despersonalizado BMP, compresión WSQ y estándar de calidad NIST Fingerprint Image Quality-NFIQ, los dispositivos de captura deben estar certificados por el FBI y con cumplir con estándares ANSI/INCITS 358-2002.

3.10.3. Seguridad tecnológica, seguridad de la información y ciberseguridad

El apartado de seguridad establece lineamientos básicos que deben cumplir estos proyectos por lo que fue subdividido en tres partes. Para iniciar, el CNTD en materia de seguridad tecnológica dispone de diez principios transversales para la seguridad tecnológica que son confidencialidad, integridad, disponibilidad, no repudio, minimizar la superficie de ataque, establecer valores predeterminados seguros, principio de privilegio mínimo, defensa en profundidad, gestión de riesgos de terceros y segregación de funciones.

De estos principios solo cabe una relación con el tema de investigación de la siguiente manera, confidencialidad, la información solo es tratada por personas autorizadas; integridad, la información solo puede actualizarse o modificarse por personas autorizadas; disponibilidad, la información es accesible al momento que se requiera, para cumplir estos tres principios se deben constituir controles que permitan a cabalidad su cumplimiento y se debe relacionar con el principio de privilegio mínimo, este indica que para poder realizar un proceso se requiera la cantidad mínima

de privilegios incluyendo “funcionalidades del sistema, permisos acceso y acciones sobre el sistema de archivos, entre otros.” (CNTD, p. 70).

Por su parte, el tema de seguridad de la información y ciberseguridad es un compendio de lineamientos básicos organizacionales sobre temas subyacentes como capacitación, recursos humanos, accesos, aplicaciones permitidas, ingresos, entre otros, esto con el fin de mantener segura la información de los administrados, a pesar de su importancia son de índole técnico más que jurídico. Por otro lado, se mencionan los estándares que debe cumplir cada proyecto, ITIL, COBIT, ISO 27001, ISO 27002, ISO 27032, ISO 22301, ISO 31000, OWASP y NIST.

3.10.4. Infraestructura y Tecnología en la Nube.

Este capítulo en tema de infraestructura habla sobre como la Administración Pública debe buscar la manera de usar la ya existente en consistencia con la realidad económica del país, eso sí esta debe interoperar entre las diferentes instituciones y debe permitir una escalabilidad a largo plazo asegurando la continuidad del servicio operando 24/7/365 con disponibilidad del 99,99% del tiempo, y todo en cumplimiento con las normativas vigentes.

Con relación a la tecnología en la nube, advierte que se debería priorizar la contratación de servicios en la nube pero que se debe realizar evaluaciones en aspectos técnicos, legales y financieros, ya que la amplitud de servicios de computación en la nube requiere estudio previo el servicio que se debería adquirir, estos con el fin de brindar un mejor y actualizado servicio. Por otra parte, este tema se debe analizar también desde la óptica de contratación pública o incluso de tercerización de servicios.

3.10.5. Interoperabilidad.

La importancia de la interoperabilidad en el futuro del Derecho Administrativo digital se plasma en este capítulo, los autores dictan que la interoperabilidad “no es un fin en sí mismo, es un medio a través del cual alcanzar un objetivo orientado a la prestación de un conjunto de servicios, apoyado por un conjunto de procesos internos de las organizaciones para facilitar los servicios (...)” (CNTD, p. 113), profundiza en el valor estratégico de este postulado y es un tema que se ha venido trabajando desde 2019 con la ayuda de ILPES/CEPAL en un proceso de interoperabilidad con 15 instituciones de la Administración Pública que conforman un volumen alto de gestiones administrativas y citando textualmente al CNTD (p.p. 113-114)

son:

1. Agencia de Protección de Datos de los Habitantes (PRODHAB)
2. Banco Central de Costa Rica (BCCR)
3. Caja Costarricense del Seguro Social (CCSS)
4. Comisión Nacional de Datos Abiertos (CNDA)
5. Dirección General de Archivo Nacional (DGAN)
6. Poder Judicial
7. Dirección General de Migración y Extranjería (DGME)
8. Ministerio de Economía Industria y Comercio (MEIC)
9. Ministerio de Hacienda
10. Presidencia de la República
11. Ministerio de Planificación (MIDEPLAN)
12. NIC Costa Rica
13. Registro Nacional

14. Tribunal Supremo de Elecciones (TSE)

15. Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT)

De la misma manera se plantea una orientación jurídica, normativa y legal que busque una cooperación interinstitucional que elimine barreras pero que se mantenga dentro del marco de legalidad. Sobre la misma línea se esboza la creación de políticas de interoperabilidad semántica y técnica; la primera se define como la capacidad que tienen los sistemas de interpretar y entender el significado de la información compartido y el segundo como la capacidad de conectarse e intercambiar esos datos.

Uno de los principales aportes de este apartado es la necesidad de catalogar la gestión administrativa en G2G (gobierno a gobierno), G2B (gobierno a empresa) o G2C (gobierno a ciudadano), esto con el fin de decidir cual información se puede acceder y cuáles son los servicios disponibles para cada una.

Es conveniente recalcar que, así como en una gestión administrativa física se debe tramitar documentos físicos y que estos se deben almacenar por un tiempo definido o indefinido, en las gestiones administrativas digitales se debe hacer lo mismo. Para resolver esta situación el CNTD además de recomendar estándares en la gestión de documentos electrónicos también hace referencia a la utilización de la Norma técnica para la gestión de documentos electrónicos en el Sistema Nacional de Archivo, Acuerdo N°7 del 25 de abril de 2018 por parte de la Junta Administrativa del Archivo Nacional.

En relación con este tema, el CNTD plantea que los documentos electrónicos deben cumplir con al menos cuatro propiedades: autenticidad, que es la atribución inequívoca del documento a la persona que afirma ser el creador; fiabilidad, que refiere al contenido del documento es “una representación completa y precisa de las actuaciones, las actividades o los

hechos de los que da testimonio" (CNTD, 2024, p. 122); integridad, que no posee alteraciones y la disponibilidad, que refiere a que el documento pueda ser "localizado, recuperado, presentado o interpretado" (CNTD, 2024, p. 122) y que pueda ser ligado y utilizado para las actuaciones por las cual fue creado y en caso de ser necesario que se almacene en un repositorio.

Sobre esta misma línea se define como debe ser el ciclo de vida del documento electrónico, y se definen tres fases:

1. Fase de captura: después de su creación, esta fase es la que indica el ingreso del documento al sistema de la gestión de documentos de la institución.
2. Fase de mantenimiento y uso: el documento una vez ya finalizada la gestión, en caso de ser un documento que mantiene su validez se debe mantener y estar disponible.
3. Fase de conservación y selección: en caso de que el documento posea validez efímera se deben eliminar por regla, según el tiempo que se determine por las autoridades.

En resumen, la gestión de los documentos es un pilar fundamental para lograr tanto la digitalización como la interoperabilidad entre las instituciones de la Administración Pública, la CNTD designa que cada institución debe ser la responsable de cada documento que capture y/o emita, manteniendo los parámetros de interoperabilidad técnica y semántica que designe la Dirección General del Archivo General (DGAG) esto con el fin que los documentos puedan ser utilizados por cualquier organización o administrado en gestiones administrativas correlacionadas. Para lograr esto la DGAG debe instituir lineamientos sobre los metadatos, tanto para su gestión, codificación, descripción y preservación.

El MICITT se encuentra en una fase de implementación del llamado Marco de Interoperabilidad Nacional, con esta visión planea desplegar nueve etapas que el CNTD (2024, p. 136) enumera así:

1. Participación, sensibilización y homologación del lenguaje.
2. Estructura y organización de la interoperabilidad.
3. Marco de interoperabilidad.
4. Modelo de interoperabilidad.
5. Identificación de la situación actual, conceptos, encuestas y métricas.
6. Definir la estrategia de la interoperabilidad.
7. Servicios de interoperabilidad.
8. Procesos de interoperabilidad.
9. Implementación de la interoperabilidad.

3.10.6. Neutralidad Tecnológica.

La neutralidad tecnológica es un término para definir que cada institución del Estado tiene la libertad para escoger e implementar la opción tecnológica que se adapte mejor a sus necesidades. Para lograr esto el CNTD implementa los principios de independencia tecnológica, interoperabilidad, libre concurrencia y competencia.

3.11. Decreto Ejecutivo N°45061-MICITT. Reglamento para la gobernanza en ciberseguridad y la resiliencia cibernética de las Instituciones Gubernamentales.

Este decreto es resultado de varias iniciativas de la Administración Pública, especialmente el Poder Ejecutivo, mediante la Estrategia Nacional de Ciberseguridad que fue creada debido a los ataques cibernéticos de 2022 que además desembocaron en la emisión de la Directriz No. 133-MP-MICITT y el Decreto Ejecutivo No. 43542-MP-MICITT, ya derogados.

En realidad, este decreto aporta lineamientos en caso de ataque cibernético que se dé una recuperación del servicio pronta y con la mínima o nula brecha en los datos. Aparte, define dentro

de la estructura organizacional del MICITT la creación de la Dirección de Ciberseguridad (DC) y que esta última también tenga bajo su dependencia al Departamento Centro de Respuesta a Incidentes de Ciberseguridad (CSIRT-CR) que en resumen es un ente de respuesta ante ciberataques, y el Departamento Centro de Operaciones de Ciberseguridad (SOC-CR) que se encarga de monitorear posibles amenazas.

3.12. Sistema de Verificación de Identidad (VID) e Identidad Digital Costarricense (IDC) del Tribunal Supremo de Elecciones (TSE)

El VID o Sistema de Verificación de Identidad es un sistema que "que permite el cotejo de la huella dactilar del ciudadano costarricense con la registrada en la base de datos del Tribunal Supremo de Elecciones a partir de su número de cédula de identidad." (Tribunal Supremo de Elecciones, s.f.)

Este servicio lo brinda el TSE a terceros, que deben pagar planes o paquetes para realizar las consultas por medio de las huellas digitales, y corroborar la identidad de la persona. El TSE también hace hincapié que por factores genéticos o externos en algunos casos no es posible realizar un cotejo exitoso de la huella digital.

El IDC o Identidad Digital Costarricense que entró a funcionar el 9 de setiembre de 2025 es la nueva herramienta digital que ofrece el TSE, actualmente con un costo de 2600 colones y una vigencia de cuatro años. A pesar de que su función es equiparable a una cédula física, al momento de su activación posee un acceso a la base de datos biométricos del TSE para asegurar una autenticación del administrado fiable.

3.13. Directrices y políticas varias

En relación con la misma temática de la digitalización, se encuentran otro tipo de cuerpos normativos y políticas públicas que también buscan generar un cierto impacto, no obstante, para el análisis de esta investigación no se consideran de gran relevancia debido a que el aporte o el impacto que brindan no es significativo. Entre estas se pueden mencionar a:

1. Estrategia Nacional de Ciberseguridad 2023-2027. La cual fue implementada por el Gobierno de la República y el Ministerio de Ciencia, Tecnología y Telecomunicaciones como un marco estratégico nacional ante los riesgos y amenazas cibernéticas producto de los ataques ocurridos durante 2022 contra las instituciones y tiene como visión que para 2027 el ecosistema digital sea confiable.
2. Directriz N° 053-H-MICITT, Regulación y normalización de adquisiciones de tecnología y/o desarrollo de sistemas informáticos, la cual indica que se deben cumplir por parte de las instituciones públicas las Normas Técnicas de la Contraloría General de la República y los lineamientos emitidos por el MICITT sobre la racionalización del uso de los recursos públicos y principalmente aquellos destinados a equipos electrónicos, programas computacionales y/o desarrollos de sistemas informáticos de apoyo a su gestión, esto según al primer artículo de esta directriz.
3. Estrategia de Transformación Digital 2023-2027: Como política pública nacional se fundamenta en la necesidad de la modernización de la Administración Pública y los sectores productivos mediante herramientas digitales como la Inteligencia digital, *big data*, robótica y computación; además destaca la importancia de la gobernanza digital, ciberseguridad e interoperabilidad como ejes transversales.

4. Plan Nacional de Desarrollo de las Telecomunicaciones (PNDT): Se plantea mediante una hoja de ruta el desarrollo de las telecomunicaciones en un rango de seis años en Costa Rica desde 2022 a 2027. Reconoce a las telecomunicaciones como un factor transversal y habilitador del desarrollo social, económico, educativo y laboral. Se aborda temas como conectividad, espectro radioeléctrico, competencias digitales, inclusión social, accesibilidad.

En conclusión, el marco normativo costarricense revela un esfuerzo legislativo significativo por dotar de validez jurídica a las actuaciones digitales de la Administración Pública, sustentado principalmente en la Ley de Certificados, Firmas Digitales y Documentos Electrónicos y la reciente creación de la Agencia Nacional de Gobierno Digital. Sin embargo, este robusto andamiaje legal padece de una fragmentación operativa, donde la coexistencia de múltiples normativas dispersas y la falta de una reglamentación técnica uniforme dificultan la implementación de una verdadera gobernanza digital integral. Si bien el derecho administrativo ha logrado evolucionar para reconocer el entorno virtual, aún persiste una brecha entre la norma escrita y su aplicación práctica, especialmente en lo que respecta a la simplificación de trámites y la plena eficiencia del servicio público.

Asimismo, se colige que el sistema normativo actual enfrenta el reto inminente de armonizar el uso de tecnologías disruptivas con la protección reforzada de los derechos fundamentales del administrado. La normativa analizada subraya que la digitalización no debe interpretarse únicamente como una herramienta de modernización, sino como un nuevo paradigma donde el principio de legalidad debe garantizar la seguridad jurídica y la autodeterminación informativa.

En este sentido, la consolidación del Derecho Administrativo Digital en Costa Rica requiere no solo de la vigencia de las leyes vigentes, sino de una reforma que centralice las competencias

de ejecución y asegure que el acceso a la tecnología sea un derecho garantizado y no una barrera burocrática adicional.

CAPÍTULO IV – ANÁLISIS DE NORMATIVA COSTARRICENSE Y DERECHO COMPARADO

El presente capítulo tiene como objetivo realizar un análisis comparativo entre el sistema normativo costarricense y los modelos digitales de Estonia y Chile, que se han seleccionado por su liderazgo y vanguardia en la implementación de la gobernanza digital. Este ejercicio de derecho comparado no pretende una simple descripción de sus plataformas tecnológicas, sino la identificación de las estructuras legales y los principios jurídicos que han permitido que estos Estados transformen la relación con sus administrados de manera eficiente, segura y transparente.

A través de este contraste, se busca extraer lecciones aprendidas y mejores prácticas que puedan ser adaptadas a la realidad nacional, analizando cómo han resuelto desafíos críticos como la interoperabilidad de datos, la identidad digital única y la ciberseguridad. Al examinar el éxito de estos referentes internacionales, se establecen las bases conceptuales necesarias para formular las propuestas de cambio normativo que se detallarán en los apartados finales de esta investigación, con el fin de robustecer el Derecho Administrativo Digital en Costa Rica.

4.1. Análisis normativo del manejo del derecho administrativo digital de Costa Rica

Desde la Constitución Política de Costa Rica (1949), se abordan dos derechos fundamentales, los cuales son el derecho a la intimidad y el derecho fundamental del acceso a la información de las telecomunicaciones.

El primero de estos derechos, se encuentra en el primer párrafo del artículo 24, el cual desenvuelve que el Estado costarricense debe garantizar que la comunicación e información debe ser íntima e indiscreta, lo cual involucra la inviolabilidad de la documentación privada hasta comunicaciones escritas y orales. Así mismo, el voto 2021 del 2003 de la Sala Constitucional, el cual realiza una interpretación de este artículo, señala que se:

> (…) garantiza a todas las personas una esfera de intimidad intangible para el resto de los sujetos de derecho, de tal forma que aquellos datos íntimos, sensibles o nominativos que un ente u órgano público ha recolectado, procesado y almacenado, por constar en sus archivos, registros y expedientes físicos o automatizados, no pueden ser accedidos por ninguna persona por suponer ello una intromisión o injerencia externa e inconstitucional (…).

En otro aspecto, es el segundo párrafo de este mismo artículo que se incorpora en 2023 debido a la reforma constitucional impuesta en la Ley N° 10385, la cual reconoce el acceso a la telecomunicación como un derecho fundamental. Durante el proceso como proyecto de ley para la modificación al artículo, el cual en un principio iba dirigido al artículo 30, pero se consideró que mejor se dirigiera al artículo 24; la Sala Constitucional en la resolución del expediente 23-002554-0007-CO del 08 de marzo de 2023, señaló la razón expuesta por los legisladores. La cual se debe a que las telecomunicaciones han incrementado y forman parte de la vida cotidiana de la sociedad, así mismo:

> (...)permite crear más empleos, así como atraer inversión a través de la incorporación de empresas, que requieren personas capacitadas con acceso a internet para mejorar la calidad de vida en algunas de las zonas alejadas y más vulnerables de nuestro país, puesto que el acceso a tecnologías de información y comunicaciones es un catalizador de la economía y la persona que no tenga acceso tiene muchas posibilidades de estar destinada a la pobreza(...).

De igual manera, la resolución anteriormente mencionada enfatiza la necesidad del Estado de incorporar este derecho fundamental en la Constitución Política, con el propósito de reafirmar la relevancia del acceso a las tecnologías de la información, más allá de lo señalado en la

jurisprudencia. Esta incorporación busca consolidar la protección constitucional de un ámbito esencial para la participación ciudadana y el ejercicio efectivo de otros derechos fundamentales.

No obstante, al tratarse de una reforma de reciente incorporación, aún no se ha desarrollado un cuerpo normativo que regule de manera integral y uniforme la actuación de la Administración Pública en relación con este derecho. Como consecuencia, se evidencia una disparidad entre las distintas instituciones públicas en cuanto a sus niveles de acceso y gestión de las telecomunicaciones, situación que suele estar condicionada por factores presupuestarios, logísticos o de localización geográfica. Asimismo, otro limitante relevante recae sobre las personas que no cuentan con el sistema de firma digital. Aunque una parte de la población económicamente activa dispone de esta herramienta, aún persisten amplios sectores que carecen de ella, tales como adultos mayores, personas con algún tipo de discapacidad, comunidades indígenas y poblaciones que residen en zonas rurales, vulnerables o de difícil acceso. Además, muchas de estas personas desconocen el uso de la firma digital y la perciben como una barrera tecnológica más que como un medio de facilitación.

La Sala Constitucional en sus resoluciones, ha señalado que las instituciones deben brindar apoyo a quienes enfrenten tales limitaciones; sin embargo, dicho acompañamiento resulta, en la práctica, insuficiente o de difícil comprensión para la población afectada. Esto se logra evidenciar por ejemplo en el voto N° 01844 de 2024, donde el motivo fue la falta de acceso a servicios básicos de telecomunicaciones —como telefonía fija, móvil e internet— en el territorio indígena de Telire en la Cordillera de Talamanca, debido a que afectaba gravemente la comunicación en casos de emergencia, el acceso a información educativa y la continuidad lectiva de los menores, la Sala Constitucional resolvió que siempre debe agotarse la vía administrativa, sin embargo al tratarse de población vulnerable, se aplica la excepción que permite conocer el fondo en sede constitucional,

y se concluyó que se "…tiene como propósito llevar telefonía e internet a zonas y comunidades donde aún no hay servicio, promoviendo acceso universal, servicio universal y solidaridad, en los términos establecidos en el artículo 24…", de igual forma, se reitera desde antes de la reforma de 2023 en votos de 2003 y 2004 que:

> Es menester que los servicios públicos atiendan la demanda de todos los administrados, sin poder alegarse razones presupuestarias o bien, limitaciones técnicas, que pueden enervar el goce y ejercicio de los derechos fundamentales inherentes o asociados a la prestación efectiva de un servicio público, tal como la libertad de comunicación. En el estado de cosas de la sociedad digital o informática y, dado el desarrollo tecnológico existente, los servicios de telecomunicaciones constituyen un servicio esencial que no puede ser negado, (…) no puede escoger su clientela o usuarios y, por consiguiente, debe brindárselo a todo el que se lo requiera.

Relacionado con las limitaciones de la firma digital, sería voto 15491 de 2017, el cual relataba sobre un agricultor de 60 años, sin conocimientos informáticos que el Registro Nacional le impedía inscribir garantías mobiliarias mediante firma física debido a que tenía que contar con la firma digital para realizar el trámite, y se reconoció por parte de la sala que:

> (…) Ello dado que la Administración debe instaurar mecanismos para que los administrados, como el amparado, puedan acudir directamente a realizar el trámite del registro de firma digital, apersonándose a las oficinas, sin incurrir en el costo económico que significa el trámite de la firma digital (…).

Esto deja en evidencia, que la herramienta de la firma digital más que generar un beneficio en la gestión pública, se entorpece incluso desde un trámite sencillo y a su vez, genera una falta al principio de accesibilidad en no poder brindarle al administrado una opción alterna para poner

realizar sus gestiones y hacerlo incurrir en un gasto innecesario en una herramienta que no le sabría dar un adecuado uso al no tener conocimiento.

Por lo anterior, es pertinente resaltar que, si bien la digitalización constituye un proceso irreversible y necesario para la modernización del Estado, no debe concebirse como una transformación radical que sustituya completamente los medios analógicos. Persisten sectores poblacionales donde el papel y la gestión administrativa tradicional siguen siendo indispensables, por lo que la transición hacia lo digital debe realizarse de manera progresiva, inclusiva y equitativa a través del tiempo.

Asimismo, la Ley General de Administración Pública establece en su cuarto artículo que el servicio público constituye una necesidad social esencial cuya adecuada prestación corresponde al Estado. En razón a esto, la digitalización cumple un papel en el cual no debe entenderse como un servicio público en sí misma, sino que un instrumento que asume y proyecta sus características. Ello obedece a que la incorporación de herramientas digitales permite facilitar principios propios de la administración pública tales como la continuidad que vela por la prestación de un servicio sin interrupciones; la universalidad que facilite el acceso superando las barreras geográficas y temporales; y regularidad donde se impulse una mayor estandarización de los procedimientos administrativos, principalmente los últimos dos, los cuales han sido más deficientes pero la transformación digital buscaría fortalecer y mejorar el acceso, estandarización y la eficiencia.

Como se logró evidenciar anteriormente, la Constitución Política y la Ley General de Administración Pública son las dos normativas principales y la base de lo que se constituye el Derecho Administrativo. Es a través de ambas que persiste el principio de reserva de ley, con la finalidad de que el gobierno bajo su responsabilidad promueva y genere normativa vinculante que facilite la integración de la digitalización y establezca de una vez el ámbito de actuación. A lo cual

se llega al siguiente cuestionamiento ¿Está Costa Rica realmente preparada para la digitalización? Con el fin de responder a esta interrogante, se deben analizar a profundizar las siguientes áreas temáticas como: Gobernanza digital y distribución de competencias institucionales, infraestructura tecnológica y ciberseguridad del Estado, protección de datos personales, identidad digital, interoperabilidad administrativa, así como lo desafíos estructurales que presenta el modelo costarricense.

4.1.1. Gobernanza digital y distribución de competencias institucionales.

Esto radica en relación con la falta de claridad en la estructura institucional y la delimitación de función entre los entes, lo cual puede generar un choque de competencias donde dos o más entes pueden competir o rechazarla. El Ministerio de Innovación, Ciencia, Tecnología y Telecomunicaciones (MICITT) fue creado bajo la ley N° 7169, la cual únicamente estipula dos artículos su finalidad y funciones generales como rector de ciencia y tecnología, mencionados anteriormente en esta investigación. Es hasta 2013 que se le atañe el sector de telecomunicaciones que pertenecía previamente al Ministerio de Ambiente y Energía.

En consecuencia, gran parte de sus atribuciones quedan sujetas a interpretación, derivadas de la amplitud de su denominación institucional en el área de digitalización al ser un concepto ligado con la innovación y tecnología que le compete al MICITT. Esta indeterminación ha provocado que el MICITT asuma un papel de amplio alcance en el impulso del avance tecnológico, sin que exista un marco jurídico que precise los límites de su competencia, generando vacíos legales, duplicidad de funciones e incluso, conflictos de competencia con otros entes públicos.

Por su parte, el Ministerio de Planificación Nacional y Política Económica o mejor conocido como MIDEPLAN, ostenta con la responsabilidad de ser el ente que vele por la

modernización y reforma de la Administración Pública y encargado de la coordinación interinstitucional.

No obstante, se puede interpretar que existe entre el MIDEPLAN y el MICITT un conflicto de competencia donde un acto administrativo enfocado a la digitalización puede ser de ambos o de ninguno, ya que no se ha discutido desde la doctrina, jurisprudencia ni mucho menos desde la ley situaciones donde ambas instituciones puedan ponerse de acuerdo sobre quien corresponder organizar a los demás entes públicos. Lo cual ha repercutido negativamente en la eficacia de las políticas públicas orientadas hacia la transformación digital, evidenciándose un estancamiento, y hasta se podría comenzar a hablar de un retroceso, en la implementación de creación de mecanismos digitales que permitan la intercomunicación de los sistemas utilizados por las instituciones.

4.1.2. Infraestructura tecnológica y ciberseguridad del Estado

La Ley General de Telecomunicaciones es quien posibilita el desarrollo de servicios digitales, sin embargo, la seguridad de dicha infraestructura ha demostrado tener cierta vulnerabilidad. A raíz de los ataques cibernéticos en los que se incurrieron en el hackeo de instituciones como la Caja Costarricense del Seguro Social y el Ministerio de Hacienda en 2022, se dictó el Decreto Ejecutivo N° 45061 del MICITT con el fin de detectar vulnerabilidades, notificar incidentes y mantener los respaldos de los datos, de manera en que se considera como un atestado en materia de ciberseguridad, no obstante, se creó de manera reactiva producto de la emergencia ocasionada.

De igual manera, es importante destacar que al tratarse de un decreto ejecutivo y no una ley formal, carece de cierta fuerza jurídica vinculante, como si se hubiese creado mediante un proyecto de ley en la Asamblea Legislativa. Además de que para fines de esta investigación no se

lograron obtener resultados sobre la eficacia y eficiencia en la funcionalidad de estos Decretos Ejecutivos.

Ante la situación estructural se encuentra inmersa la política exterior en relación con la implementación del 5G, esto debido a que "tiene como fundamento el control y suministro ilimitado de información a la alta velocidad que constituyen la base para inteligencia artificial" (Estado de la Nación, 2025, pp. 276-277), lo cual ha generado controversias según los intereses de Estados Unidos por la influencia de la República Popular de China en la región, considerando además que la empresa Huawei obtuvo las licitaciones para las redes 3G (2009) y 4G (2011).

Ante estas presiones, el presidente Rodrigo Chaves firmó el Decreto Ejecutivo 44196-MSP-Micitt, que regula la ciberseguridad en servicios 5G y superiores, donde en el inciso c del artículo 10 estipula que los vendedores o proveedores potenciales deben haber adoptado la Convención de Budapest sobre el Cibercrimen, mismo que el país asiático no ha ratificado. Mismo decreto generó un recurso de amparo a la Sala Constitucional debido a que "el decreto regulaba materia que debía ser conocida por la Asamblea Legislativa y no por el Ejecutivo, así como discriminatorio por violar los principios de libre competencia e igualdad de participación de las empresas en concursos públicos" (p. 276), a lo cual, la Sala resolvió que esto debía ser competencia del Tribunal Contencioso Administrativo.

No obstante, esta situación deja una problemática debido a que un tema de carácter técnico en busca de una solución benefactora a la ciudadanía y como principal sujeto dentro de esta investigación: a la Administración Pública, asume cualidades geopolíticas que impiden que exista un adecuado desarrollo y apertura a las nuevas tecnologías. Esto debido a que el 5G busca brindar una mayor funcionalidad para la Administración Pública al brindarle una más amplia interconexión permitiendo cumplir con el principio de universalidad, asimismo velaría por darle

solución a problemáticas como la falta de cobertura que se evidencia ante un sistema ya vegetativo y fuertemente obsoleto, del cual, ya el país se está enfrentando.

4.1.3. Protección de datos personales.

Los operadores de telecomunicaciones o la red, que principalmente son instituciones públicas, tienen la potestad de guardar datos de ubicación y navegación, en el primer caso la pueden utilizar sin individualizarla y sólo para fines relacionados con el mejoramiento de servicios, sobre los datos de navegación los operadores si la pueden individualizar para asuntos de facturación. En este último, es importante indicar que los datos deben ser suprimidos cuando se cancela o se extingue el servicio, pero la ley no determina o no fiscaliza si realmente esos datos llegan a ser borrados en algún momento ni mucho menos el administrado tiene conocimiento de ello.

La Ley de Protección de la Persona frente al tratamiento de sus datos personales Nº 8968, en su tercer artículo señala las definiciones propias de datos irrestrictos, restringidos y sensibles, sin embargo, lo hace de una manera genérica y no profundiza en el manejo y el control dependiendo de cada acto administrativo.

Se presenta, por consiguiente, una ausencia hacia los datos biométricos, donde no se ha definido si pertenecen a ser datos sensibles o restringidos y donde se debe asegurar que estos datos deben ser actualizados y veraces, lo que deja vacíos en materia de protección legal y responsabilidad institucional.

De forma reciente se han creado bajo decreto ejecutivo organizaciones enfocadas en la revisión de programas y su verificación, como es el caso de la Agencia Nacional de Gobierno Digital, no obstante, al ser muy reciente no ha habido resultados contundentes de trabajo como para determinar su veracidad.

4.1.4. Identidad y certificación digital

El desarrollo de la firma digital y la certificación electrónica representa uno de los avances más sólidos del marco jurídico costarricense. La Ley de Certificados, Firmas Digitales y Documentos Electrónicos establece un sistema que garantiza la autenticidad e integridad de los documentos digitales, con base en estándares internacionales.

El proceso implica la acreditación de los entes certificadores ante el ECCA, bajo la supervisión del MICITT. El Banco Central de Costa Rica funge como certificador principal mediante el uso de infraestructura segura y sistemas como el SINPE Móvil, que opera con claves públicas y privadas.

Esta normativa es una de las más robustas del ecosistema digital, sin embargo, su rigidez técnica ha generado tensiones con la expansión de nuevos servicios digitales, ya que constituye prácticamente la única herramienta jurídica que asegura la verificación de identidad digital con respaldo legal pleno, no obstante, esto no evita que sea inflexible y retrasa aún más la transformación digital.

Además, como se mencionó anteriormente, llega a obligar al ciudadano a tener una firma digital debido a las limitaciones en la identificación, lo cual los hace incurrir en un gasto que puede llegar a ser hasta innecesario, ya que muchas personas no tienen conocimiento en su uso y tampoco es una herramienta que vayan a utilizar con frecuencia. Por lo cual la Firma Digital, cada vez deja de ser una herramienta facultativa a ser obligatoria para realizar cualquier gestión de carácter administrativo. Lo cual no es negativo, pero la transformación hacia la digitalización debe pensarse desde un enfoque paulatino y progresista velando una mejor integración para las poblaciones mayores que no tienen habilidades en la sociedad.

4.1.5. Interoperabilidad administrativa

Lo que se busca con el principio de interoperabilidad es que cada institución tenga definida su competencia en relación con la información y los datos que maneja, de manera que cada institución sea quien brinda la información que se requiera para un trámite sin necesidad que sea el administrado que deba aportarla. Esto mismo promueve el tema de la ciberseguridad debido a la sectorización de datos como ocurre en diversos países, y donde independientemente de la situación, Costa Rica está inmerso o vulnerable que pueda nuevamente ocurrir un fallo o un hackeo en cualquier momento.

En Costa Rica, la interoperabilidad como concepto, ya estaba proyectado desde 2002 con la Ley de Protección al Ciudadano frente al Exceso de requisitos y trámites administrativos mediante el uso de un tipo de ventanilla digital, pero la ausencia de un sistema integrado y seguro a impedido su materialización adecuada. Mediante el documento de identidad o cédula, se pueda realizar una serie de trámites en conjunto sin necesidad de trasladarse.

Se requiere de una neutralidad tecnológica de manera que toda documentación o información permanezca dentro de un mismo formato que sea accesible para los distintos sistemas y programas que emplean las instituciones públicas. Mismos sistemas que son creados bajo el principio de discrecionalidad administrativa, debido a la falta de leyes con descendientes que formalicen el sistema digital y que impide que el país no genere un avance significativo de importancia en lo que transformación digital se refiere.

4.2. Derecho Comparado

El siguiente apartado desarrolla un análisis de derecho comparado de los modelos normativos avanzados de dos países indicando diferencias y buenas prácticas normativas aplicables al contexto

costarricense. Para ello, se examinan los ordenamientos jurídicos de Estonia y Chile, seleccionados por su grado de avance, coherencia institucional y reconocimiento en procesos de transformación digital del Estado. Estonia representa un modelo consolidado de gobierno digital que ha sido modelo y el ejemplo a nivel internacional con una estructura normativa flexible y altamente interoperable, por otro lado, Chile constituye un referente regional con una estrategia gradual y sistemática de modernización administrativa que todavía se encuentra en proceso de transformación. El estudio comparado de ambos casos permite evaluar cómo distintos marcos jurídicos han abordado la digitalización administrativa y extraer criterios útiles para el fortalecimiento del Derecho Administrativo Digital en Costa Rica.

4.2.1. Estonia

La República de Estonia, es un Estado ubicado en Europa Oriental y cuenta con una población aproximada de un millón ciento noventa y cuatro mil habitantes (CIA, 2025). Formó parte de la Unión de Repúblicas Socialistas Soviéticas (URSS) de forma forzosa desde 1940 hasta su disolución en 1991. Desde entonces, forma parte de organismos internacionales de relevancia como la Unión Europea, Tratado del Atlántico Norte (OTAN) y la Organización para la Cooperación y el Desarrollo Económicos (OCDE), donde en este último también se encuentra Costa Rica como miembro desde 2021.

En el aspecto jurídico, Estonia se encuentra en la familia romano-germánica, igual que el país centroamericano, no obstante, Margaret Makk (2021) señala que el derecho estonio actual se encuentra influenciado por otros sistemas jurídicos.

> Additionally, generally recognized principles of international law and binding international treaties form an inseparable part of Estonian law. Judicial precedent (…) is decisive with regard to issues of interpretation of law or when gaps in legislation need to be bridged.

> (…). Note, however, that the Estonian legal system is formally norm-based, not a mixed system of precedent and statutory law. Interpretation of norms is necessary to allow the legal system to keep pace with a rapidly changing modern society.
>
> The classical distinction between private and public law is somewhat difficult nowadays. (…). Under this principle, legal norms aimed at protecting the interests of the weaker party are usually imperative, so that agreements entered into in contravention of these principles are void (Makk, 2021).

En relación con la cita anterior, se evidencia como el sistema jurídico estonio, más allá de la norma formal y escrita, de la cual es la base fundamental según lo estipula el artículo tercero de su Constitución (1992), ha requerido de otras fuentes interpretativas para fortalecer su normativa como la jurisprudencia ante el cambio social al que se encuentra inmerso. Ante esto, en el análisis comparado con Costa Rica, se debe examinar si dicha flexibilidad normativa ha tenido un desarrollo enfocado a la luz de la digitalización y la transformación administrativa del Estado.

Con la recuperación de su independencia, Estonia comenzó un proceso de reconstrucción del Estado que implicó la elaboración de una nueva Constitución y el establecimiento de un sistema institucional desde sus raíces. Este panorama proporcionó al país la posibilidad de desvincularse de las estructuras burocráticas convencionales y adoptar un modelo de Administración Pública enfocado en la digitalización. Esta decisión no solo se enfocó en el aspecto moderno y futurista de la época, sino también la digitalización constituía la opción más factible y económica.

En 1998, según mencionan Krõõt & Mikiver (2024) se establecieron los "Principios de la política de información de Estonia", lo que facilitó lo siguiente bajo tres principios esenciales:

1. La actualización de las leyes para alcanzar una sociedad de la información eficiente y operativa.

2. Soporte para el crecimiento del sector privado.

3. Optimizar el vínculo entre el Estado y los ciudadanos a través de la concienciación e información a la población acerca de los progresos y oportunidades de las soluciones de Tecnología de la Información.

En esta misma línea, las autoras señalan que en el año 2000 se desarrolló el sistema de gobierno electrónico para agilizar la administración pública y el proceso de toma de decisiones gubernamentales ágil y sin papel, donde cualquier ciudadano puede consultar a cualquier hora y con actualización en tiempo real; además de la posibilidad de declarar los impuestos en línea y en 2005 se introdujo el voto electrónico, siendo el primer país del mundo en hacerlo. De manera que, en Estonia, los únicos trámites que se deben realizar presencialmente son los matrimonios, divorcios y compras de bienes inmuebles (2024).

En la conferencia expuesta por Marten Kaevats sobre "¿Qué es un gobierno y una sociedad Digital?" señaló lo siguiente: "In Estonia we have very few digital laws that work with technicalities because digital technologies changed fast so if you encode those into legal systems then you are building a legacy system that is not adaptable towards the future" (CongresoAmericaDigital, 2019, m19s20), esto quiere decir, que Estonia no se requiere instaurar leyes donde se expliquen detalles técnicos, ya que la ley se queda limitada ante el constante cambio de la tecnología, de lo contrario, quedarían obsoletas y sin poderse adaptar al futuro. Por eso, prefieren leyes más generales o flexibles, que puedan mantenerse vigentes y adaptarse al futuro sin necesidad de estarse reformando constantemente. Inclusive se podría comenzar a considerar que el uso excesivo de leyes, como se acostumbra en el sistema legal estructurado, como un riesgo de crear un sistema de gobernanza paralela que puede en lugar de flexibilizar la digitalización, la podría llegar a bloquear.

Dicha ley entró en vigor en 2001, y tiene como propósito según dispone su primer artículo, es garantizar el acceso a la información de acceso público con base a los principios de un Estado democrático y social de derecho; dicha información es la obtenida o creada en el ejercicio de las funciones públicas, por lo cual no aplica para aquella que se considera de secreto de estado o información extranjera clasificada, se prevé que el acceso a la información sea gratuito a menos que existan costos de suministro, donde en ese caso, se darán a conocer las condiciones de acceso y las tarifas, que no deben ser restrictivas (Riigi Teataja, 2025a). Posteriormente en los artículos 11 y 28 señalan que esta ley introdujo la obligatoriedad de que todas las instituciones estatales del Estado mantuvieran un registro de todos los documentos públicos en internet (Riigi Teataja, 2025a; Krõõt & Mikiver, 2024).

Acceso de datos de información. En primer lugar, conviene a destacar la separación entre las definiciones de datos abiertos y cerrados, según lo que ya dispone esta ley.

Los datos abiertos son de uso general, no están restringido por ley y que puede ser reutilizados, esto quiere decir que se puede dar uso con fines comerciales o no comerciales diferentes del propósito original, ya estas contribuyen al interés público e inclusive si estas brindan algún tipo de beneficio como al medio ambiente y la economía, se pueden acceder digitalmente sin condiciones.

En el artículo 4, señala que la información se facilitará en un archivo estructurado y legible de forma digital, de manera que las aplicaciones de software puedan identificar, reconocer y extraer fácilmente datos específicos, y se debe poner a disposición del público sin restricciones a la reutilización del documento con una descripción de los datos que tiene. En el caso de que no pueda ser legible digitalmente, el usuario que la proporciona debe facilitar el acceso a los datos abiertos en su formato original o en cualquier otro formato (Riigi Teataja, 2025a).

A diferencia de estos, los datos cerrados deben garantizar la privacidad del usuario, la protección de los derechos de autor, la seguridad nacional, los secretos comerciales y cualquier otra información de acceso restringido. De previo a brindar información de forma general, el usuario deberá evaluar si existe la necesidad imponer restricciones del uso general de sus datos.

De dicha manera, se logra evidenciar como Estonia regula el ingreso y acceso a la información, de manera que diversas instituciones públicas puedan dar uso de esta de forma sencilla y eficaz, siempre y cuando se vele por la seguridad y la privacidad del usuario, y previéndole a este que puede brindar restricciones, con el fin de evitar que la apertura genere riesgos en la esfera personal, patrimonial o estratégica.

De este modo, la relación entre datos abiertos y cerrados revela una doble dimensión: por un lado, la necesidad de garantizar la máxima accesibilidad posible a la información de interés público, y por otro, la obligación de proteger datos sensibles cuya divulgación podría vulnerar derechos fundamentales o comprometer intereses colectivos. En el caso de la información que contiene datos personales restringidos por ley o por algún tipo de procedimiento igualmente regulado, no se pondrá en conocimiento público, y en el caso de que sea parcial, sólo se dará a conocer aquella información que, si es de acceso público siempre que no haya un riesgo de revelar datos protegidos, y si contuviera datos personales se debe hacer de manera que no cause un daño significativo, por lo que se anonimiza nombres y direcciones.

Principios de acceso a la información pública. El artículo 4 de la ley señala que es esencial para un Estado democrático y el garantizar derecho y deberes, las instituciones públicas tienen la obligación de dar el acceso a la información. Donde este acceso, el cual es gratuito (salvo que exista una tarifa, la cual debe ser pública, explicable, razonable y no discriminatoria), debe ser rápido, sencillo, brindar protección a la privacidad de las personas y los derechos de autor. Se

permite también que cualquier persona pueda impugnar restricciones de acceso si considera que están violando sus derechos (Riigi Teataja, 2025a).

Basándose en el principio de interoperabilidad, se permitió el trabajo en conjunto de distintas bases de datos, la cuales están reguladas en otras normas como lo han sido ley de registro de población, registro de la propiedad, registro mercantil y antecedentes penales (Krõõt & Mikiver, 2024). Por dar un ejemplo, el registro de población, según lo define el Ministerio del Interior de Estonia (2025), es una base de datos de los nacionales y ciudadanos de la Unión Europea que se les haya otorgado derecho de residencia; lo que se pretende es que la información que se utilice sea para el cumplimiento de las funciones públicas de manera que simplifique la tramitaciones, mejore las funcione del Estado y puede garantizar una gestión más fluida en el ámbito administrativo, esto claramente, conforme a la ley y los límites establecidos, ya que esta información tiene un efecto jurídico por la utilización que constituye.

Titulares, solicitantes y procedimiento acceso de la información. En el caso de los titulares, la ley se refiere a las entidades estatales y municipales, personas jurídicas dentro del derecho público, privados y particulares cuando desempeñen funciones públicas sobre la base de una ley, un acto administrativo o un contrato, incluida la prestación de servicios públicos educativos, sanitarios, sociales u otros servicios públicos, con respecto a la información que se refiere al desempeño de estas funciones, y también a empresas con monopolio natural, en relación con sus precios y condición de servicios.

La solicitud, por otro lado, es cuando toda persona (sin interés legítimo específico) como solicitante pide acceso de la información al titular, y en este caso el acceso se puede dar mediante dos formas: por solicitud de que la persona pide la información o por divulgación cuando la

institución la pública sin que alguien lo solicite. Incluye también el derecho a reutilizar datos abiertos, respetando las licencias cuando existan (Riigi Teataja, 2025a).

Esta tramitación se encuentra regulada a partir del artículo 13, donde se señala que dicha solicitud puede ser tramitada de forma oral directamente o por teléfono, así como por escrito mediante un correo, fax o correo electrónico, lo que permite que el solicitante no requiera ejercer el trámite de forma presencial ante la institución a la que requiere la información, sino que puede hacerlo digitalmente.

En dicha solicitud debe indicar las calidades de la persona física o jurídica, los datos de contacto para hacerle llegar la información al solicitante y el contenido o tipo de información que está solicitando como el nombre, contenido del documento o detalles conocidos del documento y el método de solicitud. Si en la solicitud existieran datos de personales restringidos, propios del solicitador, la institución pública deberá identificar la persona y si fueran de un tercero los datos debe informarle sobre el fundamento y la finalidad del acceso a la información (Riigi Teataja, 2025a). Es importante destacar que esto es un tratamiento que compone un derecho de la ciudadanía, por lo que no puede verse como un privilegio personal en el caso de que alguien intente ampararse en su cargo oficial o laboral.

Dentro del aspecto de la accesibilidad, el artículo 15 en adelante hace mención de que es una obligación del titular de la información, es decir, en este caso la Administración Pública explicarle el procedimiento, requisitos y métodos desde la ubicación y el medio para acceder a la información. Las solicitudes se registran al momento de su recepción o como máximo un día hábil después y deben gestionarse en un plazo máximo de 5 días hábiles, y si son casos de mucha complejidad se puede extender a 15 días, lo que demuestra la rapidez de su gestión, donde se incluye los datos del solicitando, el funcionario que lo va a tramitar y el plazo de respuesta. No es

necesario registrar una solicitud de información si es anónima, se presenta de forma oral, o por vía electrónica y se atiende de forma inmediata.

La información debe entregarse en la forma solicitada: digital, copia en papel, fax, oral -en el caso que sean consultas simples-. inspección presencial u otros medios; si no puede ser de esa forma, se debe buscar otro que el solicitante pueda, y si no se define, se elige el más adecuando, siendo este probablemente el digital, según la cotidianeidad del país. También, si fuera el caso de que el titular no tiene competencia para brindar la información, debe hacerle saber al solicitante e indicarle a donde deberá referirse o enviar inmediatamente una solicitud de información por escrito al competente.

El solicitante puede pedir copias oficiales o certificadas cuando las necesite para ejercer derechos u obligaciones. Se da por cumplido el acto administrativo cuando: se entrega la información en la forma prevista, se remite a la institución competente de la información y el solicitante puede acceder a ella. Asimismo, puede darse la negativa por cumplir y esto puede ocurrir en los casos de que la información esté restringida y quien solicita no esté autorizado, el titular no posee la información y no sabe quién la tiene, no se ha cancelado la tarifa que se solicita; y puede ser facultativa en el caso de que la información ya fuese entregada, no se vincula al ejercicio de las funciones públicas, implica un volumen excesivo de información que afecte las funciones del ente, requiere sistematización o análisis que generan nueva información y puede ser que el solicitante tiene capacidad jurídica limitada o no proporciona datos de contacto. En todo caso, la negativa debe notificarse en máximo 5 días hábiles, con justificación.

Como medio se utiliza un portal nacional único, el cual es: *Eesti.ee*, y es mediante la identificación digital que se le brinda al ciudadano, este puede ingresar a los datos que el gobierno tiene a disposición, así como verificar la integridad de la información que las instituciones

(públicas o privadas) han manipulado o utilizado, esto según Kaevats, permite que la ciudadanía estonia sea dueña de su propia información (CongresoAmericaDigital, 2019, m23s15).

En relación con el control y manejo de la información por parte de la sociedad estonia, también es importante destacar el papel que juega el X-ROAD y el principio “Only Once”, que se encuentran estipulados en el artículo 43 y siguientes de esta ley y de los cuales se profundizará posteriormente.

En relación con la supervisión del cumplimiento de esta ley, es velado por la Inspección de Protección de Datos, la Oficina del Sistema de Información del Estado (RIA), la Oficina de Estadística y la Oficina de Protección al Consumidor y Supervisión Técnica; donde se busca el cumplimiento de las solicitudes, divulgación, protección de datos, así como la gestión de bases de datos. Si hubiese la violación de algún derecho, se puede presentar una denuncia ante estas autoridades o el tribunal administrativo (Artículo 44, Riigi Teataja, 2025a,).

4.2.1.1. La Ley de Procedimiento Administrativo.

Esta es la ley principal que regula el ámbito de la Administración Pública en Estonia, cumpliendo un papel equivalente a la Ley General de la Administración Pública en el ordenamiento costarricense. A partir del artículo 3, establece como principio la protección de derechos donde los derechos y libertades fundamentales pueden ser restringidos en virtud de la ley. El derecho de discreción, en el artículo 4, es donde se le otorga a una autoridad administrativa el uso de la información del cual se deben respetar los límites autorizados y la finalidad de dicha discrecionalidad, la accesibilidad donde la autoridad es responsable de proporcionar información sobre los procedimientos administrativos ya sea de forma física o digital ya que deben ser públicos y de manera accesible para las personas, la protección información de secretos estatales y

comerciales se mantiene de forma confidencial y sobre la protección de datos se regula mediante el Reglamento de la Unión Europea 2016/679, según señala el inciso 2 de este mismo artículo.

Es importante señalar a que se define como autoridad administrativa según esta ley y su artículo 8, como cualquier organismo o funcionario facultado para desempeñar las funciones, establecen normas para determinar la jurisdicción y recusación de funcionarios en caso de conflicto de intereses. Además, se menciona a los participantes en los procedimientos administrativos, en el artículo 11, las cuales se refiere a los solicitantes, destinatarios, terceros afectados y autoridades que deben emitir opiniones o aprobaciones para la emisión de un acto jurídico o medida, de igual manera, en el segundo inciso señala que se pueden involucrar a otras personas y organismos que puedan verse afectados por una decisión, contrato o medida administrativa.

En el artículo 5 inciso 6 y artículo 14 inciso 4 disponen que todo procedimiento electrónico tendrá las mismas calidades que si fuese escrito y que toda solicitud tramitada se le añadirá las firmas digitales y los sellos electrónicos con sus debidas especificaciones (Riigi Taetaja, 2024a).

Asimismo, según el artículo 27, los documentos tramitados estarán en disposición en el sistema o portal de información o se enviarán por correo electrónico con su debida firma digital, o dependiendo del caso con sello electrónico. En el caso del acto administrativo, más allá de que debe ser clara e inequívoca como señala el artículo 55, este mismo artículo en su inciso tercero y cuarto señalan que:

> (3) An administrative decision in writing may be issued in electronic form. The requirements set for written administrative decisions apply to electronic administrative decisions, taking into account the specifications arising from the electronic form of documents.

> (4) A written administrative decision shall set out the name of the administrative authority which issued it, the name and signature of the head of the administrative authority or a person authorised thereby, the time of issue of the administrative decision and other information prescribed by a legal act. A digital signature need not be added to an electronic administrative decision if the head of an administrative authority or a person authorised [sic] thereby can be identified in a secure manner. (Riigi Taetaja, 2024a)

Por lo cual, al igual que los tramites o documentos electrónicos, el acto administrativo es válido en su formato electrónico o digital e inclusive no requiere de firmas siempre y cuando se identifique legalmente a la persona o la autoridad correspondiente garantizando que un tercero no haya generado una alteración. Asimismo, la notificación se puede realizar mediante correo u otros medios electrónicos con su respectiva firma digital o sello electrónico.

4.2.1.2. Protección de datos y la Ley de Ciberseguridad

Debido a la complejidad del sistema internacional y la globalización, lo digital o cibernético son el principal blanco en ataques y hackeos, ante esto y la gran evolución que ha tenido, Estonia se ha posicionado también como un líder en ciberseguridad, esto posterior a un ataque proporcionado por Rusia en 2007 fortalecieron las defensas digitales del país debido a la necesidad de la digitalización, y generando un cambio de enfoque a nivel global de la necesidad de esta defensa (Holm, 2025). La ley de Ciberseguridad se adoptó en 2018, y aunque aparenta enfocarse en cuestiones de información sensible, defensa militar internacional, su finalidad conforme a sus primeros dos artículos se enfoca en la seguridad de los sistemas de información de las plataformas digitales de la sociedad y el sector público.

Dicha ley, en el artículo 6 dispone de principios para Garantizar la ciberseguridad donde destacan los principios de personalidad y protección integral donde el proveedor de servicios, el

cual según los numerales 3, 7 y 8 se refieren a quienes controlan y procesan sistemas de los servicios vitales como salud, transporte, bancos y Administración pública como tribunales, gobiernos locales, servicio electoral, parlamento, auditoría nacional, entre otros organismos públicos.

Estos proveedores, están obligados y tienen la responsabilidad a organizar la seguridad, identifica posibles amenazas y aplica medidas organizativas y técnicas adecuadas. También está el principio de reducción de Impacto Nocivo donde en el caso de incidente cibernético, se deben tomar medidas para evitar su propagación y notificar a la autoridad de supervisión y el principio de cooperación donde las partes interesadas cooperan en la garantía de la ciberseguridad y la resolución de incidentes. (Riigi Taetaja, 2024b) En el caso en que se llegase a presentar un incidente, el proveedor debe informarle a la Oficina del Sistema de Información del Estado, el cual es el ente competente ante estos casos; de forma inmediata o máximo dentro del plazo de 24 horas de haberse tenido conocimiento y que este incidente genere una afectación severa en la seguridad o en la continuidad de servicios.

El proveedor debe hacerle informar al público afectado, sino la Oficina del Sistema de Información del Estado lo hará según el artículo 8 incisos 5 y 6 y presentar un informa a la Oficina sobre el incidente, ya se maneja un registro para su análisis, envío de alerta y supervisión, los cuales son de acceso restringido y son de uso interno.

En relación con la supervisión según dispone el artículo 14, La Oficina de Protección al Consumidor y Supervisión Técnica, se encarga de certificar la ciberseguridad del proveedor por lo que realizan una supervisión en dicho ámbito velando por una mayor seguridad tanto para los sistemas como para las personas usuarias del mismo sistema. Asimismo, la Oficina del Sistema de Información del Estado realiza la supervisión estatal y administrativa en el cumplimiento de

requisitos, donde se puede restringir el uso o acceso de un sistema para prevenir una amenaza inminente o eliminar una violación a la ciberseguridad.

4.2.1.3. Reglamento de la Unión Europea 2016/679

Más allá de la normativa nacional, el país ha integrado en su ordenamiento jurídico las disposiciones de la Unión Europea y se conoce como el Reglamento General de Protección de Datos. Por lo cual, la protección de datos se encuentra regulado mediante dicho normativo según estipula el artículo 2 de la Ley de Procedimiento Administrativo. En su primer artículo indica como objeto la protección de las personas físicas en el tratamiento de datos personales y su libre circulación, así como la protección de derechos y libertades, en relación con los principios fundamentales donde (Parlamento Europeo & Consejo de la Unión Europea, 2016, art. 5):

1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; (…)

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten

> exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, (…) sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas (…) a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);
>
> f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).
>
> 2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

Esta normativa tiene un ámbito de aplicación, según su artículo 2, para los tratamientos automatizados total o parcialmente, así como aquellos que no lo sean pero que formen parte de un fichero o estén destinados a serlo, y es excluyente en caso de seguridad nacional, política exterior, entre otras.

Es importante destacar el artículo 9, en cual dispone de los tratamientos de categorías especiales de datos, donde se prohíbe el tratamiento de datos personales que revelen:

> el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales [sic] de una persona física.

No obstante, se tiene como excepción cuando exista: un consentimiento explicito, necesidades en el ámbito laboral y de seguridad social, protección de intereses vitales, actividades legítimas de ciertas asociaciones sin ánimo de lucro, datos hechos públicos por el interesado,

formulación de reclamaciones legales, razones de interés público esencial, medicina preventiva o laboral, salud pública, y fines de archivo, investigación científica o histórica o estadísticos (Parlamento Europeo & Consejo de la Unión Europea, 2016, art. 9).

De manera, que los datos personales de los usuarios, siempre cuando cumpla con las necesidades estatales y esté dentro del régimen del interés público o interés mayor, puede ser de uso. Con base a esto último se debe destacar los derechos del interesado, donde como principal se encuentra el Derecho a la información, donde se debe informar sobre su identidad, fines de tratamiento, destinatarios, plazos de conservación, existencia de derechos (rectificación, supresión, oposición, portabilidad) y decisiones automatizadas, lo que brinda una mayor transparencia, que también es considerado como un derecho dentro de la normativa.

Entre otros derechos se encuentran el de acceso, rectificación, olvido, oposición, entre otros. Los cuales brindan al usuario facilidades como la confirmación si están tratando o accediendo sus datos, corregir datos inexactos o completar los que hagan falta, que los datos lleguen a ser suprimidos cuando ya no sean necesarios para el fin en el que fueron recopilados, si se retira el consentimiento o se opone al tratamiento de los datos personales, y también existe el derecho a no ser objeto de decisiones basadas en el tratamiento automatizados sin intervención humana que produzcan efectos jurídicos o le afecten significativamente, esto según el artículo 22 en el inciso primero, donde también cuenta con excepciones en su segundo inciso de:

2. El apartado 1 no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas

> adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o c) se basa en el consentimiento explícito del interesado.
>
> 3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.
>
> 4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

En síntesis, la prohibición de las decisiones automatizadas no aplica en caso de celebración o ejecución no un contrato entre el usuario y la institución pública, en consentimiento explícito del usuario. Además de que la institución o el responsable a tratar con los datos personales del usuario debe salvaguardar los derechos, libertades e intereses legítimos de este, debido a esto último, los artículos 24 al 39, además el considerando 71 de este Reglamento dispone que dicho responsable debe tener:

> en cuenta las circunstancias y contexto específicos en los que se tratan los datos personales, (…) debe utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, aplicar medidas técnicas y organizativas apropiadas para garantizar, en particular, que se corrigen los factores que introducen inexactitudes en los datos personales y se reduce al máximo el riesgo de error, asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para los intereses y derechos del interesado y se

impidan, entre otras cosas, efectos discriminatorios (Parlamento Europeo & Consejo de la Unión Europea, 2016).

Lo cual este reglamento lo que busca es salvaguardar la integridad del usuario.

4.2.1.4. X-ROAD y principio "Only Once"

No se puede realizar un análisis sobre el Gobierno Digital, sin mencionar a grandes rasgos, como este se implementa y cuál es el uso que se le da en la sociedad estonia en su cotidianeidad. En primer lugar, es importante indicar, que, a nivel mundial, la gran mayoría de los países en la ya están implementando herramientas como parte de los proyectos de digitalización y automatización de la Administración Pública, sin embargo, utilizan mecanismos de alto costo y segregados de forma independiente.

Como bien menciona Eaves & McGuire (2019), cada servicio depende de su propio y extenso sistema de software; en el cual cada persona en cada trámite desde su licencia de conducir o ir al banco, se debe brindar su información personal de forma reiterada desde su número de identificación, domicilio, correo electrónico que si desean actualizar deben hacerlo uno por uno; ya que los sistemas que se implementan no convergen la información entre sí, por lo cual los sistemas lo único que llegan a almacenar es la recopilación información reiterada, lo que genera mayores costos y un manejo de depósito de datos que podría utilizarse para otras cosas.

De igual forma, estos autores en su artículo "Lessons from Estonia on digital government" sobre cómo Canadá también está aprendiendo las políticas aplicadas en Estonia, señalan que esto genera también que los ciudadanos o usuarios de estos sistemas se vean confundidos, lo que genera que no los quieran utilizar, lo cual no es su propósito, esto sin mencionar que las actualizaciones son lentes o nunca se dan por lo que dificulta la innovación a tal punto que la puede imposibilitar.

Estonia en cambio, tiene un sistema llamada X-ROAD, el cual su objetivo era la creación de una solución técnica donde una autoridad estatal pudiera utilizar los datos de otra para la realización de sus tareas sin crear una super base de para todos los datos recopilados (Krõõt & Mikiver, 2024). Desde 2001, ha trabajado en los siguientes requerimientos: Interoperabilidad, Integridad de datos, privacidad; por lo cual los datos atraviesan de forma sencilla los diferentes sistemas sin alteración y encriptada previendo la seguridad de los usuarios. Esto ha generado en Estonia eficiencia en la eliminación papeleo redundante, acceso instantáneo a la información y que los funcionarios públicos se enfoquen en tareas significativas que requieren de criterio humano (Lars, 2024)

De manera que todas las bases encuentran independientes, pero estos pueden intercambiarse entre sí, ya que son de acceso libre para las instituciones gubernamentales de una forma segura, por ejemplo, si se diera alguna situación de investigación de la cual la policía requiere información, esta tiene acceso al historial médico, fiscal e incluso mercantil de la persona (Lars, 2024). De dicha forma, la persona puede acceder a los diferentes sitios web gubernamentales, ya que entre las bases de datos se comparte de la información de manera que, si se hace una modificación u actualización de información, todas las bases de datos se actualizan de forma automática, y siempre brindando al usuario un registro de quién y cuando se realizaron esas modificaciones.

Conforme a lo dispuesto, la Administración Pública tiene la obligación de requerir al usuario la información solicitada únicamente en una ocasión. Este mandato responde al denominado principio Only Once, cuyo propósito es suprimir la exigencia de que los ciudadanos deban proporcionar de forma reiterada los mismos datos a las distintas instancias administrativas. El artículo 43.3 de la Ley de Información Pública (PIA), en el inciso 2, señala que está prohibido

establecer bases de datos independientes para la recopilación de los mismos datos, por lo cual se queda sustentado legalmente dicho principio. De igual forma, el artículo 43.8 indica que son de acceso público siempre y cuando la ley disponga lo contrario.

Por otro lado, este principio y el sistema X-ROAD también ha trascendido fronteras, de manera que ya se ha ido aplicando en países como Finlandia e Islandia y posteriormente se ha buscado implementar dentro de la Unión Europea en su Estrategia para el Mercado Único Digital, donde también hay críticas debido a que podría reducir el control de los ciudadanos sobre sus datos, por lo cual se pretende que los datos sean recopilados únicamente para fines explícitos y legítimos (Lars, 2024; Krõõt & Mikiver, 2024).

4.2.1.5. Lecciones de Estonia

Basado en el artículo del panel "Building Resilient and Effective Digital Societies-Lessons and Opportunities" expuesto por Marcus, Kask, Lauringson, Ilves y Sild (e-Estonia, 2023) durante La Cumbre Digital de Tallin, capital de Estonia, podemos señalar, en síntesis, importantes puntos de los cuales el país báltico se ha convertido en un ejemplo en el área del desarrollo digital administrativo.

En primer lugar, desarrollo habilidades digitales de una forma muy temprana (Década de 1990) por lo cual inculcó o fomentó competencias digitales en la sociedad antes que se comenzaran a digitalizar los servicios formalmente y no sería hasta los 2000 que introduciría el X-ROAD. Por otro lado, en el caso de Costa Rica esto se puede ejemplificar con la implementación de una educación digital y tecnológica, donde en los centros de primaria y secundaria del Ministerio de Educación Pública se les brindó a los estudiantes equipos tecnológicos para fortalecer el aprendizaje en distintas regiones del país mediante la Fundación Omar Dengo durante 30 años

hasta 2023 y posteriormente el Programa Nacional de Formación Tecnológica en 2024 (CONARE, 2025 pp.44-45).

Como segundo punto, Estonia veló por la obligatoriedad de la identidad digital como clave para su éxito, donde Toomas Hendrik Ilves, presidente de la República de Estonia (2006-2016) señaló que "digitisation [sic] efforts had failed to coalesce in countries where such identities were optional, as people weren't motivated to use an optional identity. Governments were similarly not motivated to create digital services" (e-Estonia, 2023), esto quiere decir que ante la falta o la poca presencia de usuarios que utilicen la firma digital, tanto para el Estado como posibles instituciones privadas que quieran formar parte de la iniciativa son capaces de notar que no llega a ser rentable invertir en la digitalización.

El tercer punto es la necesidad política, debido a que debe existir un compromiso por implementar reformas, ya que hay gobiernos que únicamente velan por la compra de equipos sin invertir en conocimiento. Además, como parte fundamental, se encuentra el marco jurídico mismo que debe ser sólido, a lo Ilves indicó que las leyes son el software de la sociedad y si la sociedad cambia también lo debe hacer el software, afirmando que Estonia no habría logrado ese marco consolidado si no hubiera adoptado a Ley de Firma Digital en el 2000 (e-Estonia, 2023). En el caso de Costa Rica, este es uno de los desafíos más persistentes.

En relación con el Marco Jurídico, Kask, directora general de Proud Engineers, expresa más allá de una innovación técnica, se requiere de una necesaria innovación legal, ya que cuando los abogados dicen no se les permite hacer nada porque la ley los limita, hay que preguntarse quien crea esas leyes, es decir, el gobierno. (Tallinn Digital Summit. 2023, m18s05).

Seguidamente se encuentra los últimos puntos de no esperar un éxito tan rápido y la exigencia de una revolución de pensamiento. En el primero de ellos, se enfoca propiamente en que

las metas no deben ser concebidas como objetivos estáticos o definitivos, debido al ritmo acelerado en el que se encuentra la sociedad y la globalización, por lo que la estructuración debe ser planteada desde un enfoque de mejora continua y adaptación permanente.

Inclusive, Estonia ha implementado nuevas iniciativas para fortalecer su sistema digital a pesar de lo consolidado que es, cosa que Costa Rica ha desatendido. Por otro lado. La resolución de pensamiento va dirigida hacia los funcionarios públicos, con el fin de familiarizarse con el cambio al gobierno digital y principalmente a países en desarrollo. Ilves también indica que:

> that digitisation has also entered an era where it is no longer focused on moving paper documents online but rethinking how to build services without a link to legacy systems. He called this perspective being a digital native and said it will require "a revolution in thought.

En síntesis, Estonia evidencia un Estado digital consolidado enfocado en una normativa amplia que vele por una visión estratégica, innovación y un compromiso hacia la constante mejora. Ante esto, Costa Rica puede aprender y beneficiarse mediante mecanismos de cooperación internacional como asesorías y capacitación para la implementación de tácticas adaptadas, de manera que el país pueda avanzar hacia un ecosistema digital coherente, resiliente y alineado con las demandas contemporáneas de la sociedad y la globalización.

4.2.2. Chile

Es un Estado sudamericano que se rige por un sistema jurídico continental basado en el derecho civil y una jerarquía normas, teniendo como norma general la Constitución Política creada 1980, y seguido a ellas están las leyes ordinarias. (Endress Gomez, 2019). Desde finales de los 90, Chile inició el proceso de transformación digital con políticas como "Chile: Hacia la sociedad de la información" (1999), la cual no tuvo tanto éxito y se formaron otras estrategias como

“Agenda Digital Chile 2004-2006” que tampoco fue tan exitosa y fue reemplaza por otras estrategias en los años 2007 y 2013, mismas que no generaron una gran continuidad debido a que no contaban con un marco de trabajo a largo plazo (Ylarri, 2025). Por lo tanto, en 2023, en colaboración con la Comisión Económica para América Latina y el Caribe (CEPAL), se impulsó una estrategia con proyección de forma gradual hasta 2027 (Ylarri, 2025).

El boletín ejecutivo 11.882, señaló la necesidad que ha tenido Chile con respecto a esta transformación nacional donde no se pretende que únicamente la digitalización brinde accesibilidad y la digitalización de trámites, sino que la tecnología es capaz de integrarse mediante la automatización de procesos, dispositivos móviles como teléfonos, compras en línea y hacer gestiones que ahorran tiempo, además de que genera un ahorro de papel genera un beneficio de carácter ambiental al Estado (2018). Lo que se pretende es que sea “implica un cambio cultural y administrativo sustancial, y no meramente traspasar a formato electrónico la actual tramitación en papel; es, después de todo, adquirir un nuevo compromiso del Estado con sus funcionarios, sus familias, y con la sociedad entera” (Boletín 11.882-6, 2018).

El ente encargado de establecer las políticas y normativas, desarrollar plataformas y orientar a instituciones en la implementación de la Transformación Digital, es la Secretaría de Gobierno Digital, creada bajo la ley 21658 se encuentra adherido al Ministerio de Hacienda desde 2024 (República de Chile, 2024c).

4.2.2.1. Ley N° 21.180 de Transformación Digital del Estado

Esta ley se publicó en 2019 y entró en vigor en 2022, donde el propósito es que se impulsen las solicitudes digitales como la normal y las presenciales sean la excepción, asimismo la modificación de diversos cuerpos normativos con el fin de plantear los estatutos enfocados a la digitalización de manera que beneficiase en tiempo, accesibilidad costos y calidad de vida de los

administrados. En conjunto, en el 2022 se realizó una reforma la cual modificó los plazos sobre la gradualidad de la implementación de la transformación digital, donde se prevé que se cumplan todos los objetivos y materias específicas hasta el 31 de diciembre del 2027 (República de Chile, 2024a).

4.2.2.2. Ley 19880 - Establece bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado

También modificó varios artículos de la ley 19.880, la cual corresponde a ser "Establece bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado", la cual en su primer artículo señala que: "La presente ley establece y regula las bases del procedimiento administrativo de los actos de la Administración del Estado. Todo procedimiento administrativo deberá expresarse a través de los medios electrónicos establecidos por ley, salvo las excepciones legales." (República de Chile, 2024a, art. 1), lo cual ya consolida el medio electrónico como la principal vía y de forma supletoria la presencia del papel en la gestión administrativa, de manera que los administrados pueden tramitar mediante un servicio en línea sin necesidad de presentarse personalmente en la instancia estatal que requiera, así como copias y notificación digitales, permitiendo una mayor cercanía con el Estado más expedita y sencilla.

En el artículo 16 se le añade un bis, lo cual dispone de una serie de principios generales sobre los medios electrónicos - como se menciona anteriormente en esta investigación, cuando se refiere al término de "electrónicos", se va a gestionar como sinónimos de "digitales"-, donde se indica que los procedimientos administrativos bajo esta modalidad deben cumplir con "neutralidad tecnológica, de actualización, de equivalencia funcional, de fidelidad, de interoperabilidad y de cooperación" (República de Chile, 2024a, art. 16 bis).

A lo cual se refieren sobre que los sistemas no deben sucumbir por obsoletos o desuso, que tengan la misma validez como si se hubiesen tramitado de forma física con sus firmas digitales respectivas, se conservarán en un expediente digital adecuado, donde se velara por la interacción, operación y cooperación entre las demás instituciones de la Administración Pública, donde el administrado no debe fungir como un intermediario brindando información de una institución pública a otra, sino que sean las mismas instituciones de forma interna que gestionen dicho trámite ya sea que la institución misma la haya generado o fuese que el administrado la aportó, lo cual se sintetiza en el ya reiterado principio de interoperabilidad.

En relación con el procedimiento administrativo per se, el artículo 18 y 19 disponen del uso obligatorio de las plataformas electrónicas y que deberá hacerse constar el procedimiento administrativo mediante un expediente digital con su respectiva fecha y documentación que presentada por los interesados que será ingresada por medios electrónicos de las plataformas de las instituciones de la Administración Pública, salvo las excepciones previstas de ley, donde si no se pudiera de esta manera, se deberá realizar el procedimiento de entrega de solicitudes, formularios y escritos mediante el papel, cuales se digitalizarán y se ingresarán al expediente digital, los cuales tendrán acceso a los interesados.

Con respecto a las notificaciones a las personas usuarias y administrados, se realizará mediante medios electrónicos según la información que exista en el registro único del Servicio de Registro Civil e Identificación, el cual contiene “domicilios digitales únicos, cuyas características y operatividad será regulada mediante reglamento dictado conjuntamente por el Ministerio de Hacienda y el Ministerio de Justicia y Derechos Humanos. Dichas notificaciones tendrán el carácter de personal”, en el caso de que no se tengan medios tecnológicos se podrá realizar mediante carta dirigida al domicilio o se recibirán en las dependencias de la instrucción pública la

cual se deberá apersonar el usuario, esto conforme al artículo 46 (República de Chile, 2024a, art. 46).

4.2.2.3. Reglamentos de Microformas (Ley 18.845) y Documentos Electrónicos y certificación (Ley 19.799)

Las microformas corresponden a ser "una imagen compactada o digitalizada de un documento original a través de una tecnología idónea para su almacenamiento, conservación, uso y recuperación posterior, conforme al artículo 1 del reglamento sobre Sistemas de Microcopia o Micro grabación de Documentos, donde se debe velar por la fiabilidad en el sentido de que, al digitalizarse el documento, este debe ser una copia fiel del documento original. Dicha microforma se debe hacer constar su recibo y estado, para posteriormente ser conservado en el archivo o registro público según corresponda y en el caso de que sea extraviado se deberá reconstruir dependiendo de la necesidad análoga que se requiera (República de Chile, 2024a, art. 3).

También es importante indicar que los documentos ya digitalizados, tendrán el mismo valor que si se tratasen como físicos y en los casos en que "los documentos originales no se hayan destruido y si hubiere diferencias entre éstos y sus microformas, se estará al documento original" (República de Chile, 2024a). Además, se podrá incurrir en la destrucción una vez transcurridos diez años si se trata de instrumentos públicos o cinco años si fueren instrumentos privados, donde previamente se publicará mediante Diario Oficial por si existiera algún tipo de interés previo a su destrucción.

En relación con los documentos electrónicos, la firma y la certificación de esta, se prevee que cumpla con los principios "de libertad de prestación de servicios, libre competencia, neutralidad tecnológica, compatibilidad internacional y equivalencia del soporte electrónico al soporte de papel", según su primer artículo de la Ley 19.799, donde los actos administrativos

otorgados entre personas ya sean físicas o jurídicas, tendrán la misma validez y producirán los mismos efectos si fuese hecho por escrito y en papel, así como la firma electrónica a la manuscrita, a menos que cumplan con las excepciones del artículo 6:

> Se exceptúan aquellas actuaciones para las cuales la Constitución Política o la ley exija una solemnidad que no sea susceptible de cumplirse mediante documento electrónico, o requiera la concurrencia personal de la autoridad o funcionario que deba intervenir en ellas (República de Chile, 2024b, art. 6).

En conjunto, a lo anterior, el artículo 8 hace mención del uso de la firma digital en la Administración Pública, en el cual se señala que no se debe restringir sin justificación a "el acceso a las prestaciones que brinden y a la publicidad y transparencia que rijan sus actuaciones y, en general, que se cause discriminaciones arbitrarias" (República de Chile, 2024b).

Además de ello, se dispone la posibilidad de contratar servicios de certificación de firmas con entidades acreditadas, en su mayoría del sector privado nacionales o extranjeras, según se considere pertinente, respalda el artículo 11 de esta ley. A diferencia de lo anterior, en Costa Rica también ofrece dicho servicio de certificación de firmas; no obstante, las entidades que prestan estos servicios son públicas, pese a que la normativa costarricense permite que dichos servicios puedan ser brindado por instituciones del sector privado.

4.2.2.4. Estándares y normas técnicas obligatorias

A raíz de esta ley, que promueve la transformación digital del Estado chileno, se establecieron se normas técnicas mediante decretos de ley por el Ministerio Secretaría General de la Presidencia y otros, con la intención de que se puede cumplir con los principios generales en los que se basa la implementación prevista a culminarse para 2027. En primer lugar, se encuentra la Norma Técnica de Autenticación, la cual establece como las instituciones del Estado deben

integrar los mecanismos de autenticación a sus plataformas institucionales con el fin de brindar seguridad jurídica a los usuarios. Seguidamente, se encuentra la de Interoperabilidad, la cual es fundamental entre la función y el servicio público promoviendo estándares, protocolos y herramientas para lograr dicho alcance.

La tercera norma es de Calidad y Funcionamiento de las plataformas, donde se pretende "mitigar la obsolescencia tecnológica, mantener la continuidad operacional, establecer y medir niveles óptimos de servicio, (…) y monitorear el óptimo estado del funcionamiento de las plataformas". Como últimas normas se encuentra la de Notificaciones, que como su nombre infiere, pretende velar por la notificación de la Administración Pública mediante el portal único creado para dicho fin, y también la norma de Documentos y Expedientes Electrónicos, que tiene como objetivo plantear estándares y formatos para la Administración Pública en relación con la gestión y administración de documentos y expedientes en su formato electrónico. Como última y no menos importante, se encuentra la Norma Técnica de Seguridad de la Información y Ciberseguridad, el cual busca definir estándares y directrices enfocadas en que las instituciones cumplan con "resguardar la confidencialidad, integridad, disponibilidad de la información y la infraestructura informática, de las plataformas electrónicas que sustentan sus procedimientos administrativos". (República de Chile, 2023 a-f)

4.2.2.5. Plataformas transversales implementadas en Chile

Se consideran los sistemas, aplicaciones o páginas digitales que utiliza el gobierno chile para la Administración Pública y los administrados. Se enfocan en tres principales ejes y es a partir de estos que desarrollan las plataformas basadas en ellas. El primer eje es "Identidad Digital Nacional", en el cual se encuentra la "ClaveÚnica", quien brinda a los ciudadanos y los residentes mayores de 14 años, el acceso a todos los servicios digitales estatales, la cual se puede solicitar

presencialmente en el Registro Civil chileno o de forma virtual en una llamada agendada previamente. El siguiente eje es “Compromiso CeroPapel”, donde se encuentra “FirmaGob”, mencionada anteriormente y creada para los funcionarios públicos para gestionar la emisión y gestión de certificados en función de las instituciones públicas.

El tercer eje se enfoca en el “Compromiso CeroFilas”, donde “SIMPLE” facilita a las instituciones digitalizar tramites de una forma rápida, sencilla, amigable y gratuita y “DocDigital” que incentiva la tramitación, envío y recepción digital de comunicaciones oficiales entre instituciones estatales.

En relación con la interoperabilidad, Chile diseñó “PISEE” y se encuentra en uso e implementación “PISEE 2.0”, una versión más actualizada, la cual permite el intercambio de datos, documentos y expediente entre instituciones públicas (Secretaría de Gobierno Digital, s.f.) Este sistema, representa un 18% de los servicios interoperados en 2016 y mediante un estudio elaborado por el mismo gobierno chileno en 2017 (Naser, 2021, p.43) destacó desde un enfoque tanto cualitativo que la interoperabilidad se relaciona con brindar servicios a los ciudadanos, que es favorable que exista un ente que sea quien gestione, fomente y apoye las iniciativas de interoperabilidad del Estado, que se instaure una normativa solida más allá de las recomendaciones y que se considera una debilidad que las plataformas dentro de la misma interoperabilidad, no puedan soportar la carga de trabajo y tengan fallas en el sistema, sin embargo, a pesar de ello, se cuenta con los recursos humanos y competencias para hacer frentes a estas situaciones.

Desde lo cuantitativo, el estudio realizado determina que son pocas las instituciones que tienen un papel en la transferencia de información, según las conexiones que poseen y por la diversidad de intercambios que realizan, y destaca según los indicadores que se aplicaron que todo depende de la importancia que aplique el Estado chileno, por lo que se recomienda fortalecer la

prioridad de la interoperabilidad por parte de las instituciones mediante políticas, normas, incentivos y herramientas.

4.2.2.6. Desarrollo de Chile.

A diferencia de Estonia, que cuenta con un sistema digital bastante consolidado con bastantes años de transformación, Chile se encuentra en un desarrollo menos avanzado a la exrepública soviética pero aun así mayor a Costa Rica. Lo más importante a destacar de Chile es que se trata de un país que ha ido desarrollando paulatinamente una estrategia de transformación digital proyectada para 2035 con apoyo de organismos internacionales como la CEPAL, Banco Interamericano de Desarrollo (BID) y la OCDE en el cual se demuestra un verdadero compromiso de la Administración Pública para lograr las metas planteadas. Donde como bien señala, el ministro de Ciencia de Chile Aldo Valle:

> La digitalización no es un fin en sí mismo, es una herramienta para hacer que nuestras instituciones sean más eficaces, cercanas, confiables y más justas para la ciudadanía. La estrategia del Gobierno Digital 2030 nos ofrece un horizonte claro, un Estado que diseña servicios digitales centrados en la persona, que gestiona sus decisiones con datos que construyen confianza y que fortalecen sus capacidades humanas junto con las tecnologías. Porque no basta con tener plataformas y sistemas modernos en un programa, la idea es que cada avance se traduzca en algo tangible para la vida de las personas.

En cuanto a las problemáticas o desafíos que implica la transformación digital y precisamente desde el área de la identificación digital, el Estado Andino ha logrado definir e identificar estas situaciones para brindar su debida mejora. Según la Estrategia de Identificación Digital, se menciona que Chile, tiene como desafíos tratar con su aún sistema análogo. Si bien la "ClaveÚnica", la principal plataforma institucional, que facilita el acceso de 1.800 trámites en

distintos organismos públicos, la normativa ha llegado a limitar a que pocas instituciones públicas y algunas privadas la puedan utilizar para la autenticación y requieren fortalecer la solidez de la seguridad y confiabilidad de la identidad digital.

Chile ante este llamado “horizonte claro”, mediante dos pilares fundamentales: “Chile conectado sin brechas” y “Chile Digitalizado”, donde le primero comprende iniciativas para garantizar el acceso de la tecnología y “asegurar que la conectividad y el desarrollo de habilidades se desplieguen con equidad y sin ningún tipo de discriminación, de acuerdo con las necesidades actuales y futuras de las personas” (Órdenes et al, 2023, p.8), mientras que el segundo, aborda la adopción de tecnologías digitales una vez se hayan logrado los niveles de desarrollo necesarios en la infraestructura digital. Asimismo, estos pilares involucran una serie de componente como la infraestructura digital, derechos digitales, digitalización de la economía y el Estado, ciberseguridad, entre otros, que fortalecen y consolidan la línea de trabajo planteada para los próximos 10 años, y donde, además, los marcos legales y estrategias normativas han sido su principal herramienta para garantizar y promover la inclusión y economía digital.

4.2.3. Conclusión de Derecho Comparado

En conclusión, el análisis del derecho comparado permite determinar que el éxito de naciones como Estonia y Chile no radica únicamente en la adopción de herramientas tecnológicas, sino en la existencia de una voluntad legislativa que prioriza la interoperabilidad y la identidad digital simplificada. Mientras que Estonia demuestra que una arquitectura de datos abierta y el principio de 'una sola vez' eliminan la burocracia redundante, el modelo chileno ofrece una ruta de transición realista para países latinoamericanos mediante la unificación de claves de acceso y la

digitalización de procesos notariales. Estos modelos confirman que Costa Rica posee una base técnica sólida, pero requiere de una evolución normativa que trascienda la simple digitalización de documentos hacia la creación de un ecosistema administrativo nativo digital que sea verdaderamente inclusivo.

Asimismo, se deduce que la principal diferencia entre el modelo nacional y los casos de éxito internacional es la centralización estratégica de la gobernanza digital. La comparación evidencia que, sin un marco jurídico que obligue a la comunicación interinstitucional y que facilite métodos de autenticación menos onerosos que la firma digital física, el avance será dispar y segmentado.

Por lo tanto, el estudio comparativo no solo sirve como referente de eficiencia, sino como una advertencia sobre la necesidad de actualizar la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales y la normativa de ciberseguridad, asegurando que el Estado costarricense pueda garantizar la confianza del administrado en la misma medida en que lo hacen las potencias digitales analizadas.

CAPITULO IV – PROPUESTAS Y CONCLUSIONES

5.1 Propuestas para implementar el Derecho Administrativo Digital

En el contexto actual, la implementación del Derecho Administrativo Digital en Costa Rica se presenta como una necesidad imperante para garantizar que la Administración Pública pueda mantener el ritmo que la sociedad a la que sirve requiere. Este capítulo tiene como objetivo presentar una serie de propuestas que buscan transformar el marco normativo y operativo del Derecho Administrativo Digital en el país. A través de estas iniciativas, se pretende no solo modernizar la administración pública, sino también fomentar una cultura de innovación y mejora continua que responda a las demandas de la ciudadanía y los desafíos tecnológicos contemporáneos.

En primer lugar, se debe aclarar que ya existe una base normativa con aplicaciones prácticas bastante sólida, aunque carece de uniformidad e interoperabilidad, y este problema se ha generado por la falta de un actor que realice directrices homogéneas dentro del diagrama organizacional de la Administración Pública. Durante el desarrollo de la presente investigación se muestra que existen multiplicidad de instituciones que se encuentran en el centro de toma de decisiones sobre asuntos de digitalización. La mayoría de estas competencias las concentra el MICITT, por obvias razones, pero se les debe sumar el PRODHAB siendo un ente adscrito al Ministerio de Justicia y Paz, el MEIC con su función de ser el ministerio encargado del Catálogo Nacional de Trámites y el MIDEPLAN siendo este último el que competente en coordinar los esfuerzos interinstitucionales.

Esta multiplicidad de actores, y una ausencia de jerarquía entre ellos, ha imposibilitado generar una visión administrativa homogénea y la aplicación de la discrecionalidad administrativa. Por ende, se debe implementar la creación de un órgano desconcentrado mínimo adscrito al

MICITT, y que su función sea el manejo y coordinación de canales digitales, tecnologías de la información (TI), gestiones administrativas digitales, ciberseguridad y demás relacionados.

Aunado a una reforma de la Ley N°8220 Protección al ciudadano del exceso de requisitos y trámites administrativos, ley que a pesar de cumplir con más de dos décadas de existencia nunca ha podido ser aplicada a cabalidad, ni crear una ventanilla única. Específicamente, reformar el artículo 11 donde designa al MEIC como rector en simplificación y obliga a toda la Administración Pública a designar en cada ente, órgano e institución administrativa a un "Oficial de Simplificación de Trámites" para crear una red "con el propósito de compartir buenas prácticas y coordinar las acciones institucionales que sean necesarias para el cumplimiento de esta ley" (Ley Protección al ciudadano del exceso de requisitos y trámites administrativos, 2002). La reforma consiste en trasladar la competencia de la rectoría al órgano desconcentrado mínimo adscrito al MICITT, cambiar la función como Rector de Gestión Administrativa Digital y la de Oficial de Gestión Administrativa Digital. Con el fin de que la red que se forma con este cambio permita que el rector dirija directrices a través de los oficiales para su incorporación sistemática, posibilitando la interoperabilidad interinstitucional y abriendo una oportunidad para lograr la ventanilla única.

Además de esta función, se pretende que el ente creado absorba al PRODHAB, la Dirección de Ciberseguridad, el CSIRT-CR, el SOC-CR y la Agencia Nacional de Gobierno Digital; con el propósito de consolidar la competencia en un solo lugar y no dispersa como se encuentra actualmente permitiendo una mejor toma de decisiones. Sumado a un uso real y práctico del Código Nacional de Tecnologías Digitales.

Seguidamente, se debe solucionar el tema de la autenticación del administrado, aplicando un sistema de "Únicamente una vez" similar al usado en Estonia. Ya que la principal razón de migrar hacia un mundo digital es evitar la presencialidad del usuario, sin embargo, la

Administración Pública actualmente solo posee la firma digital como medio de autenticación 100% digital, y ante los demás casos, la Administración dispone al administrado al menos iniciar el trámite *in situ* para verificar su identidad. El Tribunal Supremo de Elecciones con su sistema VID (Sistema de Verificación de Identidad, por sus siglas), sumado a los sistemas de seguridad de la cédula de identidad física pueden fungir como ente autenticador, esto con el fin de que a la hora de tramitar la documentación de identidad física se pueda generar un usuario digital o inclusive que este se ligue a la Identificación Digital Costarricense (IDC) que ya posee acceso a los datos biométricos del administrado para una autenticación segura. Y que puede funcionar como un token, clave dinámica u OTP (One-Time Password) para hacer ingresos o realizar gestiones. En el caso de personas extranjeras, se debe implementar un sistema que esté dispuesto por la Dirección General de Migración y Extranjería. Las aplicaciones o sitios web de la Administración Pública deben de utilizar este sistema para permitir acceso a sus servicios y plataformas dejando atrás la presencialidad y la firma digital como medio autenticador.

Sobre otra línea, se debe minimizar el uso de herramientas que pertenezcan completamente a terceros, por razones técnicas no se puede prescindir completamente de estos, pero al menos la plataforma principal debe pertenecer a la Administración Pública, impidiendo así generar afectaciones en caso de extinción o suspensión de los contratos.

Se debe hacer una reforma que actualice la Ley de protección a la persona frente al tratamiento de sus datos personales N° 8968, ya que no hace mención sobre el tratamiento de datos que se ha desarrollado debido a la *big data* y que como esta puede ser usada dentro del Derecho Público, y que respecto a las bases de datos sujetas al Derecho Administrativo, se debería estipular mediante ley escrita bases de datos por competencia y cuáles son las instituciones encargadas de resguardar y tratar estos datos, solo podrán compartir estos con las demás en los casos que

ameriten. Por ejemplo, la Caja Costarricense de Seguro Social es la única que puede mantener una base de datos con la información médica o el Poder Judicial con la situación jurídica. Esto no solo con el fin de que las bases de datos públicas estén bajo un órgano competente si no que, en caso de un hackeo de información, la información este fraccionada entre distintos actores y no pueda ser obtenida de manera íntegra.

En conclusión, la implementación del Derecho Administrativo Digital en Costa Rica es esencial para modernizar la Administración Pública y responder a las demandas tecnológicas y ciudadanas contemporáneas. La creación de un órgano desconcentrado adscrito al MICITT, encargado de coordinar los canales digitales y la ciberseguridad, junto con la reforma de la Ley N°8220 y la Ley de protección de datos personales, permitirá una administración más eficiente y segura. Además, la adopción de un sistema de autenticación digital robusto y la minimización del uso de herramientas de terceros fortalecerán la infraestructura digital del país. Estas iniciativas no solo mejorarán la interoperabilidad interinstitucional, sino que también fomentarán una cultura de innovación y mejora continua en el sector público.

5.2.Conclusiones

La presente investigación ha permitido realizar un análisis integral del Derecho Administrativo Digital en Costa Rica, logrando cumplir de manera satisfactoria con el Objetivo General de analizar el marco normativo nacional y contrastarlo con el derecho comparado para generar propuestas de implementación sólidas. Se ha evidenciado que la digitalización en la Administración Pública no es una mera actualización tecnológica, sino una transformación estructural irreversible que impacta directamente en la validez del acto administrativo y en la relación jurídica entre el Estado y el ciudadano.

El análisis demuestra que, si bien existen esfuerzos significativos, el país enfrenta un estancamiento normativo frente a la velocidad del cambio tecnológico, lo que genera una inseguridad jurídica que debe ser resuelta mediante una reforma profunda y centralizada.

En primer lugar, basado en el primer objetivo específico, se logró identificar y señalar una amplia gama de instrumentos legales que, aunque dispersos, constituyen la base del derecho digital actual en Costa Rica, donde se destaca: La Constitución Política, específicamente en la reciente reforma del artículo 24; la Ley General de Administración Pública cuyos principios de legalidad y eficiencia se interpretan enfocados en el concepto o la lógica digital. También se abarcan leyes como la Ley de Certificados, Firmas Digitales y Documentos Electrónicos (N°8454) y la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (N°8968), y normativas recientes como la Ley de Creación de la Agencia Nacional de Gobierno Digital (N°9943) y el Código Nacional de Tecnologías Digitales. Lo cual esta compilación destaca un sistema disperso, donde la falta de una ley centralizada que abarque la digitalización como “un solo”,

Se concluye que esta compilación revela un sistema de "normativa por parches", donde la falta de una ley marco centralizada provoca que cada institución avance a ritmos distintos, generando una fragmentación que afecta al administrado.

En segundo lugar, basado en el segundo objetivo específico se estimó dicho marco normativo en diferentes pilares de interés destacando lo siguiente: En gobernanza digital se encuentra un conflicto de competencias entre instituciones y dispersión de autoridades, que impide una estandarización de los servicios públicos digital; la protección de datos se encuentra en vulnerabilidad en el manejo de datos biométricos y sensibles, donde también el uso obligatorio de la firma digital, si bien es robusto, se ha convertido en una barrera de acceso que contraviene el principio de accesibilidad universal, excluyendo a los ciudadanos que no cuentan con este dispositivo; Por otra parte, la interoperabilidad en Costa Rica es deficiente, debido a que obliga al administrado la entrega de la misma información múltiples veces, lo que ignora el principio de eficiencia administrativa.

Como tercer objetivo, se encontraba el análisis comparado de países con modelos avanzados que han implementado el Derecho Administrativo Digital. Estonia, es considerado como el modelo de referencia y su éxito radica en la arquitectura X-Road y en la aplicación estricta del principio “Only Once” y donde las leyes deben ser el "software de la sociedad"; si la sociedad cambia, la ley debe actualizarse para permitir la innovación legal, no solo técnica. Por otro lado, Chile representa un modelo de transición gradual pero firme. Su enfoque en la "ClaveÚnica" y los pilares de "Chile Conectado" y "Chile Digitalizado" ofrece un ejemplo de cómo cerrar la brecha digital mediante un compromiso estratégico de largo plazo y políticas de Estado, más que de gobierno.

Como último objetivo específico, se plantean propuestas concretas que superan la visión simplista de "digitalizar el papel" para pasar a una "nativización digital" de la administración, entre las propuestas se puede mencionar lo siguiente: La Creación de un Órgano Desconcentrado que sea adscrito al MICITT, con competencias reales para unificar la gobernanza y supervisar la ciberseguridad y los canales digitales; Reforma a la Ley 8968 para incluir el tratamiento de Big Data y el uso de inteligencia artificial en el sector público, asegurando que el Estado sea el garante y no una amenaza para la privacidad; Implementar métodos de identidad digital más accesibles que la firma digital física, similares a la ClaveÚnica chilena, para garantizar que la digitalización no sea un factor de exclusión.

En conclusión, la investigación demuestra que Costa Rica posee la base técnica y un marco normativo inicial aceptable, pero carece de la voluntad estatal y la coherencia legal para dar el salto definitivo hacia un Estado Digital, donde también la digitalización ha avanzado de manera "natural" y discrecional.

Para que el Derecho Administrativo Digital sea una realidad efectiva, el Estado debe dejar de invertir únicamente en hardware y empezar a invertir en "innovación legal". Solo mediante un marco jurídico unificado, que priorice la interoperabilidad y la protección de los derechos fundamentales en el entorno virtual, podrá Costa Rica garantizar una Administración Pública que sea verdaderamente un servicio al ciudadano y no un obstáculo burocrático digitalizado.

Bibliografía

Academia Play. (2019) *La Revolución Industrial en 7 minutos.* [Archivo de video]. YouTube. https://www.youtube.com/watch?v=3LQAnFEADl4

Acceso a la Justicia. (s.f.) Acto Administrativo Electrónico. En *Diccionario Jurídico.* Recuperado el 30 de octubre de 2025, de https://accesoalajusticia.org/glossary/acto-administrativo-electronico/#:~:text=Es%20aquella%20declaraci%C3%B3n%20de%20voluntad,a%20trav%C3%A9s%20de%20medios%20electr%C3%B3nicos.

Aliaga Pizarro, L. (2022). Transformación Digital y Gobierno: propuesta de programa de mejoramiento de gestión para el sector público. Disponible en https://repositorio.uchile.cl/handle/2250/187915

Amazon Web Services. (s.f.) ¿Qué es la ciberseguridad? https://aws.amazon.com/es/what-is/cybersecurity/

Arroyo Chacón, J. (2013). Marco jurídico-administrativo del Gobierno Digital en Costa Rica. Revista de Derecho, Comunicaciones y Nuevas Tecnologías, 10. https://www.profesorajenniferarroyo.com/images/documentos/derecho/Administrativa/Marco_jur%C3%ADdico-administrativo_del_gobierno_digital_en_Costa_Rica.pdf

Banco Central de Costa Rica (s.f.) *Firma Digital*. https://www.bccr.fi.cr/firma-digital

Barrantes, R. (2014). Investigación: Un camino al conocimiento: Un enfoque cuantitativo y cualitativo. San José: EUNED.

Barrio, M. (2024). Manual de Derecho Digital 3a Edición. Tirant lo Blanch. https://costarica.tirantonline.com/cloudLibrary/ebook/info/9788410715301

Boletín N° 11.882 -06. (2018). Proyecto de ley, iniciado en mensaje de S. E. el presidente de la República, que modifica la Ley que establece Bases de los Procedimientos Administrativos, en materia de documentos electrónicos.

Chen, M. (2024). *¿Qué es el big data?* Oracle Latinoamérica. https://www.oracle.com/latam/big-data/what-is-big-data/

Chiriac, L., & Blaj, S. B. (2019). The Electronic Administrative Act. *Juridical Current*, *22*(2), 72–78.

CongresoAmericaDigital. (2019). *¿Qué es un gobierno y una sociedad digital? Caso de éxito de Estonia, conferencia Marten Kaevats* [Video]. En YouTube. https://www.youtube.com/watch?v=H8CZF22nD5g

Constitución Política de Costa Rica [C.P] Artículos 11, 24. 8 de noviembre de 1949. (Costa Rica) http://www.pgrweb.go.cr/scij/busqueda/normativa/normas/nrm_texto_completo.aspx?nValor1=1&nValor2=871

Cortés Abad, Óscar. (2020). La Administración tras el coronabreak. Políticas para ¿un nuevo paradigma administrativo? *Gestión Y Análisis De Políticas Públicas*, (24), 6–23. Https://doi.org/10.24965/gapp.i24.10811

Cruz Romero, R. (2017). Gobernanza digital en Costa Rica: un análisis de propuestas. *E-Ciencias De La Información*, *8*(1), 1–18. https://doi.org/10.15517/eci.v8i1.29808

Decreto Ejecutivo N°33018 de 2006. [Poder Ejecutivo]. Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos. 21 de abril de 2006.

Decreto Ejecutivo N°37554 de 2013. [Poder Ejecutivo]. Reglamento a la Ley de protección de la persona frente al tratamiento de sus datos personales. 5 de marzo de 2013.

Decreto Ejecutivo N°44507-MICITT de 2023. [Ministerio de Ciencia, Tecnología y Telecomunicaciones]. Código Nacional de Tecnologías Digitales. 19 de junio de 2024. https://www.micitt.go.cr/sites/default/files/GobernanzaDigital/CNTD.pdf

Decreto Ejecutivo N°44636 de 2024. [Poder Ejecutivo]. Reglamento de Creación de la Agencia Nacional de Gobierno Digital. 30 de agosto de 2024.

Diaz Romero, B. (2024). La transformación digital del Estado y el derecho a la protección de datos personales. *Gobierno Y administración pública*, (7), 15-27. https://doi.org/10.29393/GP7-2DEDR10002

Digital Ware. (s.f.) *¿Qué son los expedientes electrónicos?* https://www.digitalware.com.co/blog/que-son-expedientes-electronicos/

Eaves, D. & McGuire, B. (2019). *Lessons from Estonia on digital government*. Policy Options. https://policyoptions.irpp.org/fr/magazines/february-2019/lessons-estonia-digital-government/

e-Estonia. (2023). Six lessons in building a digital society. https://e-estonia.com/6-lessons-in-building-a-digital-society/

Endress Castro, S. (2019). *Essential Issues of the Chilean Legal System*. GlobaLex | Foreign and International Law Research. https://www.nyulawglobal.org/globalex/chile1.html

Euskal Estatistika Erakundea. (s.f.) *Web.* https://es.eustat.eus/documentos/opt_0/tema_423/elem_9087/definicion.html#:~:text=La%20World%20Wide%20Web%20(telara%C3%B1a,accesibles%20a%20trav%C3%A9s%20de%20Internet.

Google Cloud. (s.f.) *¿Qué es la inteligencia artificial o IA?* https://cloud.google.com/learn/what-is-artificial-intelligence?hl=es-419

Gordillo, A. (Ed.). (2016). Tratado de derecho administrativo y obras selectas: Tomo 3, El acto administrativo (10.ª ed.). Fundación de Derecho Administrativo. Recuperado de http://www.gordillo.com/pdf_tomo3/capitulo7.pdf

Granados, G. (2025). Parquímetros en San José volverán a partir de esta fecha: Esto es lo que debe saber. *CR Hoy*. https://crhoy.com/nacionales/parquimetros-en-san-jose-volveran-a-partir-de-esta-fecha-esto-es-lo-que-debe-saber/

Hernández Sampieri, R. (2023). *Metodología de la Investigación Plus*. McGrawHill - Plus. https://www-ebooks7-24-com-uh.knimbus.com:443/?il=34866

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2006). *Metodología de la investigación* (4a. ed.). McGraw-Hill.Holm, P. (2025) El enfoque audaz de Estonia en materia de ciberseguridad: un modelo holístico para Europa. E-Estonia. https://e-estonia.com/estonias-cyber-security-model-for-europe/

Husain, O. (16 de marzo de 2023). *Definición de privacidad digital: ¿Qué es la privacidad y la seguridad digital?* Enzuzo. https://www.enzuzo.com/blog/digital-privacy-definition

IBM. (s.f.) *¿Qué es el hardware informático?* https://www.ibm.com/mx-es/think/topics/hardware

IBM. (s.f.) *¿Qué es la interoperabilidad?* https://www.ibm.com/mx-es/think/topics/interoperability

Information System Authorithy. (2024). *Data exchange layer X-tee*. RIA. https://www.ria.ee/en/state-information-system/data-exchange-platforms/data-exchange-layer-x-tee

Instituto Nacional de Estadística y Censo. (2023) *Evolución en el uso de telecomunicaciones en Costa Rica.* https://inec.cr/noticias/evolucion-el-uso-las-telecomunicaciones-costa-rica

Jinesta Lobo, E. (2001) *Tratado de Derecho Administrativo Tomo I.* Biblioteca Jurídica Dike

Kaspersky. (s.f.) *¿Qué son las cookies de Internet?* https://www.kaspersky.es/resource-center/definitions/cookies

Krõõt Tupay, P., & Mikiver, M. (2024). *Public Digitalisation in a legal perspective*. Nordic Council of Ministers. https://pub.norden.org/temanord2024-503/estonia.html

Lars, E. (2024). *X-Road*. E-Estonia. https://e-estonia.com/solutions/interoperability-services/x-road/

Lenovo (s.f.) *¿Qué es un software?* https://www.lenovo.com/mx/es/glosario/que-es-software/?orgRef=https%253A%252F%252Fwww.google.com%252F&srsltid=AfmBOorXHAPrkiUkp3rp1Ipc7bYxy5XeomqXk3p9rr1VyLKOjmaqIu0J

Ley 5525 de 1974. Ley de Planificación Nacional. 13 de marzo de 1974. Colección de leyes y decretos Semestre 1 Tomo 2 Página 875

Ley 6227 de 1978. Ley General de la Administración Pública. 1 de diciembre de 1978. Diario Oficial la Gaceta N°102

Ley 7169 de 1990. Promoción Desarrollo Científico y Tecnológico y Creación del MICYT (Ministerio de Ciencia y Tecnología). 1 de agosto de 1990. Diario Oficial La Gaceta N°144

Ley 7600 de 1996. Ley de Igualdad de Oportunidades para las Personas con Discapacidad. 29 de mayo de 1996. Diario Oficial La Gaceta N°102

Ley 8220 de 2002. Ley de Protección al ciudadano del exceso de requisitos y trámites administrativos. 11 de marzo de 2002. Diario Oficial La Gaceta N°49

Ley 8454 de 2005. Ley de Certificados, Firmas Digitales y Documentos Electrónicos. 13 de octubre de 2005. Diario Oficial La Gaceta N°197.

Ley 8642 de 2008. Ley General de Telecomunicaciones. 30 de junio de 2008. Diario Oficial La Gaceta N°125

Ley 8968 de 2011. Ley de protección de la persona frente al tratamiento de sus datos personales. 5 de setiembre de 2011. Diario Oficial la Gaceta N°170.

Ley 9046 de 2012. Traslado del Sector Telecomunicaciones del Ministerio de Ambiente, Energía y Telecomunicaciones al Ministerio de Ciencia y Tecnología. 31 de enero de 2013. Diario Oficial La Gaceta N°146

Ley 9943 de 2021. Creación de la agencia nacional de Gobierno Digital. 11 de mayo de 2021. Diario Oficial La Gaceta N°187

Ley 9971 de 2021. Ley de Creación de la Promotora Costarricense de Innovación e Investigación. 28 de mayo de 2021. Diario Oficial La Gaceta N°102

Makk, M. (2021). *Estonian Legal System and Legal Research*. GlobaLex | Foreign and International Law Research. https://www.nyulawglobal.org/globalex/estonia1.html#Section_1_1

Microsoft. (s.f.) *¿Qué es la protección de datos?* https://www.microsoft.com/es-mx/security/business/security-101/what-is-data-protection#:~:text=La%20protecci%C3%B3n%20de%20datos%20se,vulneraci%C3%B3n%20y%20p%C3%A9rdida%20de%20datos.

Ministry of the Interior - Republic of Estonia. (2025). *Population Register*. Siseministeerium. https://www.siseministeerium.ee/en/activities/population-procedures/population-register

Moderne, F. (2025). Principios generales del derecho. Legitimidad, método y controversias en derecho administrativo y constitucional (pp. 65-66). Editorial Tirant Lo Blanch. https://costarica.tirantonline.com/cloudLibrary/ebook/info/9788410713925

Monforte, E. (s.f). *Datos biométricos: qué son y para qué se utilizan.* Camerfirma. https://www.camerfirma.com/datos-biometricos-que-son-para-que-se-utilizan/

Naciones Unidas (s.f.) *Gobierno electrónico.* https://publicadministration.un.org/egovkb/en-us/Overview

Naser, A. (2021). *Gobernanza digital e interoperabilidad gubernamental: una guía para su implementación*. https://repositorio.cepal.org/entities/publication/f5dc5a25-b6ec-4d77-930c-7644523c11f8

Oficina de Industria y Seguridad. (s.f.) *Entity List.* Departamento de Comercio de los Estados Unidos. https://www.bis.gov/entity-list

Órdenes, X., Robert, R., Rojas, F., & Rojas, P. (2023). *Estrategia de transformación digital: Chile Digital 2035*. https://repositorio.cepal.org/entities/publication/5017db4c-7be4-41d1-8635-0c1174976142

Parlamento Europeo y Consejo de la Unión Europea. (2016, 27 de abril).

Piñar Mañas, J. L. (2011) *Administración electrónica y protección de datos personales.* [Monografía, Estudios sobre la modernización administrativa, Dereito Monográfico] *s.n.* https://minerva.usc.gal/rest/api/core/bitstreams/4c86cf46-17de-40ae-b462-c9d5d80f63fd/content

Poder Judicial. (s.f.) Autodeterminación Informativa. En *Diccionario Usual del Poder Judicial.* Recuperado el 31 de octubre de 2025, de https://diccionariousual.poder-judicial.go.cr/index.php/diccionario/derecho-de-autodeterminaci%C3%B3n-informativa

PowerData (s.f.) *Metadatos, definición y características.* https://www.powerdata.es/metadatos

Quirós Orozco, P. E. (2025). *Orientaciones básicas para reformas en la estructura organizacional de la administración pública*. MIDEPLAN. https://biblioteca.mideplan.go.cr/cgi-bin/koha/opac-detail.pl?biblionumber=6494

REAL ACADEMIA ESPAÑOLA: *Diccionario de la lengua española*, 23.ª ed., [versión 23.8 en línea]. <https://dle.rae.es> [08 de octubre de 2025].

REAL ACADEMIA ESPAÑOLA: *Diccionario panhispánico del español jurídico*. Recuperado el 12 de enero de 2026 de https://dpej.rae.es/lema/administraci%C3%B3n-p%C3%BAblica

Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos). Diario Oficial de la Unión Europea, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

República de Chile. (2023a). *Establece norma técnica de autenticación* (Decreto N° 9). Ministerio Secretaría General de la Presidencia. Diario Oficial de la República de Chile. https://www.diariooficial.interior.gob.cl/publicaciones/2023/08/17/43629/01/2361373.pdf

República de Chile. (2023b). *Establece norma técnica de documentos y expedientes electrónicos para la gestión de procedimientos administrativos* (Decreto N° 10). Ministerio Secretaría General de la Presidencia. Diario Oficial de la República de Chile. https://www.diariooficial.interior.gob.cl/publicaciones/2023/08/17/43629/01/2361374.pdf

República de Chile. (2023c). *Establece norma técnica de notificaciones* (Decreto N° 8). Ministerio Secretaría General de la Presidencia. Diario Oficial de la República de Chile. https://www.diariooficial.interior.gob.cl/publicaciones/2023/08/17/43629/01/2361372.pdf

República de Chile. (2023d, 17 de agosto). *Establece norma técnica de interoperabilidad* (Decreto N° 12). Ministerio Secretaría General de la Presidencia. Diario Oficial de la República de Chile. https://www.diariooficial.interior.gob.cl/publicaciones/2023/08/17/43629/01/2361371.pdf

República de Chile. (2023e). *Establece norma técnica de calidad y funcionamiento de las plataformas electrónicas que sustentan procedimientos administrativos en los órganos de la Administración del Estado* (Decreto N° 11). Ministerio Secretaría General de la Presidencia. Diario Oficial de la República de Chile. https://www.diariooficial.interior.gob.cl/publicaciones/2023/08/17/43629/01/2361375.pdf

República de Chile. (2023f). *Sumario de la edición N° 43.629 del Diario Oficial* (Sumario). Ministerio Secretaría General de la Presidencia. Diario Oficial de la República de Chile. https://www.diariooficial.interior.gob.cl/publicaciones/2023/08/17/sumarios/43629.pdf

República de Chile. (2024a). *Establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado* (Ley Nº 19 880). Ministerio Secretaría General de la Presidencia. Biblioteca del Congreso Nacional de Chile. https://www.bcn.cl/leychile/navegar?idNorma=210676

República de Chile. (2024b). *Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma* (Ley Nº 19 799). Ministerio de Economía, Fomento y Reconstrucción. Biblioteca del Congreso Nacional de Chile. https://www.bcn.cl/leychile/navegar?idNorma=196640

República de Chile. (2024c). *Crea la Secretaría de Gobierno Digital en la Subsecretaría de Hacienda, y adecúa los cuerpos legales que indica* (Ley Nº 21 658). Ministerio de Hacienda. Biblioteca del Congreso Nacional de Chile. https://www.bcn.cl/leychile/navegar?idNorma=1200907

Riigi Taetaja. (2024). *Administrative Procedure Act*. Riigiteataja.Ee. https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/505122023003/consolide

Riigi Taetaja. (2024). *Cybersecurity Act*. Riigi Taetaja. https://www.riigiteataja.ee/en/eli/519082024019/consolide

Riigi Teataja (2025). *Avaliku Teabe Seadus.* Riigiteataja.Ee. https://www.riigiteataja.ee/akt/105072025003

Romero-Pérez, J. E. (2014). El acto administrativo: apreciaciones generales. *Revista De Ciencias Jurídicas*, (45). https://doi.org/10.15517/rcj.1981.15333

Secretaría de Gobierno Digital. *(s.f.) Transformación Digital del Estado, mejores servicios para las personas*. Secretaría de Gobierno Digital. Recuperado el 27 de agosto de 2025 de https://digital.gob.cl/transformacion-digital/hoja-de-ruta/

Secretaría de Gobierno Digital. (s.f.). *Plataformas Transversales*. Secretaría de Gobierno Digital. Recuperado el 06 de septiembre, 2025 de https://digital.gob.cl/plataformas-transversales/

Siles, A. (26 de enero de 2025) Agencia Nacional de Gobierno Digital inició funciones tras constituir Junta Directiva. *Ameliarueda.com.* https://ameliarueda.com/noticia/agencia-nacional-gobierno-digital-inicio-funciones-constituir-junta-directiva-noticias-costa-rica

Spacarotel, G. (3 de febrero de 2020). *Origenes del Estado y del Derecho Administrativo.* Centro de Información Jurídica

https://cijur.mpba.gov.ar/files/bulletins/Dr._Gustavo_Spacarotel__Origenes_del_Estados_-_03-02-2020.pdf

Susnjara, S. & Smalley, I. *¿Qué es el Cloud computing?*. IBM. https://www.ibm.com/es-es/think/topics/cloud-computing

Tallinn Digital Summit. (2023). TDS 2023: Panel: Building Resilient and Effective Digital Societies - Lessons and Opportunities [Video]. In *YouTube*. https://www.youtube.com/watch?v=QgxaJHjdgyI

Tribunal Supremo de Elecciones. (s.f.) *Sistema de Verificación de Identidad.* Tribunal Supremo de Elecciones. https://www.tse.go.cr/verificacion_identidad.htm

Tullocks Abarca, J. A. (2024). Análisis crítico sobre la gestión administrativa del sector público costarricense. *RESPaldo: Revista Internacional En Administración De Oficinas Y Educación Comercial*, *9*(2), 41-51. https://doi.org/10.15359/respaldo.9-2.4

UC Berkeley. (s.f.) *What is digital accesability? https://dap.berkeley.edu/web-a11y-basics/what-digital-accessibility*

Valero Torrijos, Julián (2014). «De la digitalización a la innovación tecnológica: valoración jurídica del proceso de modernización de las Administraciones Públicas españolas en la última década (2004-2014)». IDP. Revista de Internet, Derecho y Política. Núm. 19, pág. 117-129. UOC. https://dialnet.unirioja.es/descarga/articulo/5582978.pdf

Viafirma (s.f.) *¿Qué es la neutralidad tecnológica? https://www.viafirma.com/es/neutralidad-tecnologica/*

World Compliance Association. (s.f.) *¿Qué es el Corporate Compliance?* https://www.worldcomplianceassociation.com/que-es-compliance.php

Ylarri, M. T. (2025) *Transformación digital en Chile: desarrollo y beneficios*. EMB Gerencia. https://www.gerencia.cl/transformacion-digital/que-es-la-transformacion-digital-y-como-se-desarrolla-en-chile/