El futuro es de todos	Gobierno de Colombia	**FORMATO MEMORIA JUSTIFICATIVA**

Autoridad originadora:	Ministerio de Tecnologías de la Información y las Comunicaciones y Ministerio de Defensa
Fecha (dd/mm/aa):	31/01/2022
Proyecto de Decreto/Resolución:	Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital

a) ANTECEDENTES Y RAZONES DE OPORTUNIDAD Y CONVENIENCIA QUE JUSTIFICAN SU EXPEDICIÓN.

A. Antecedentes y razones de oportunidad y conveniencia que justifican la expedición de los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital.

La gestión de la seguridad digital de un país supone fortalecer muchas capacidades, que permitan identificar y gestionar los riesgos derivados de la cada vez mayor dependencia de todas las actividades económicas y sociales en el Ciberespacio.

Para el efecto, es esencial que el país avance y consolide estas capacidades, mediante la adopción de un modelo de gobernanza de la seguridad digital, la identificación de infraestructuras críticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital.

A continuación se desarrolla la justificación y las razones que motivan la expedficion de estos lineamientos:

1. En material de Gobernanza de Seguridad Digital:

El Gobierno de Colombia expidió la Política Nacional de Confianza y Seguridad Digital (Documento CONPES 3995 de 2020) que tiene como objetivo principal establecer medidas para desarrollar la confianza digital a través de la mejora de la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

Según el diagnóstico presentado en dicho documento de política pública, el marco de gobernanza en materia de seguridad digital en el país no ha alcanzado un grado de desarrollo adecuado y no ha podido lograr una adecuada interacción e identificación entre las múltiples partes interesadas alrededor del tema, generando escenarios de desarticulación y duplicación de esfuerzos, así como una baja cohesión y coordinación para dar respuesta a incidentes y a contener amenazas que se den en el entorno digital.

Teniendo en cuenta lo anterior, con miras a poder avanzar en acciones que permitieran superar lo evidenciado en el diagnóstico, el Gobierno de la República de Colombia, realizó gestiones ante la Organización de Estados Americanos – OEA, con la que sucribió el Convenio Interadministrativo 981 de 2020 a través del Ministerio de Tecnologías de la Información y las Comunicaciones -Ministerio TIC-, obteniendo con éste un acompañamieto técnico en la estructuración e implementación de acciones estratégicas de la mencionada política pública, entre ellas, la estructuración oficial de un Modelo de Gobernanza de Seguridad Digital en el país, con el que se pueda resolver la problemática descrita.

La seguridad digital requiere de la participación conjunta de multitud de partes interesadas que intervienen en todo el ecosistema de ciberseguridad y ciberdefensa en el país, desde proveedores de software, terminales y equipos, hasta los clientes finales y usuarios, tanto en el ámbito público (fuerzas armadas, gobierno, policía, etc.) y en el ámbito privado, desde los ciudadanos privados hasta las corporaciones multinacionales. Para garantizar la mayor probabilidad de éxito frente a las amenazas digitales es fundamental identificar los distintos arreglos formales e informales que determinan cómo se deben tomar decisiones públicas y cómo se deben llevar a cabo las acciones públicas, así como promover la coordinación, cooperación y colaboración más estrechas posibles bajo un modelo de gobernanza que tenga en cuenta los beneficios de la Cuarta Revolución Industrial en el futuro.

Un modelo de gobernanza, generalmente soportado bajo el enfoque de múltiples partes, es una estructura de gobierno que busca reunir a los interesados para participar en el diálogo, la consulta, la toma de decisiones y la implementación de soluciones a problemas u objetivos comunes. El principio detrás de tal estructura es que, si todas las partes interesadas en un problema, una pregunta o una inquietud proporcionan suficiente información, la eventual decisión consensual gana más legitimidad y, por lo tanto, refleja mejor un conjunto de perspectivas en lugar de una única fuente de validación.

Colombia ha venido haciendo esfuerzos muy importantes por disponer de una institucionalidad adecuada, así como como de instancias que faciliten la gestión de riesgos de seguridad digital. En las últimas políticas relacionadas con seguridad digital se han incorporado acciones que reconocen el papel relevante que tiene un enfoque de múltiples partes interesadas y se propuso la generación de mecanismos e instrumentos orientados a elevar su participación efectiva en la gestión de riesgos de seguridad digital, sin embargo, los mismos no han logrado aún la cohesión ni integración esperada y, por lo tanto, la materialización de este enfoque es un reto vigente para el país.

El diagnóstico efectuado en el documento CONPES 3995 de 2020, fue complementado en el estudio efectuado por la OEA, con los siguientes resultados:

ASPECTO	SITUACIÓN ACTUAL
Visión nacional y estratégica	No existe aún una visión estratégica nacional que se haya definido de forma participativa y, por lo tanto, compartida por todas las partes interesadas ni mecanismos para su orientación.
Liderazgo	Se ha dado un impulso a las temáticas de seguridad digital con liderazgo de la Consejería para Asuntos Económicos y Transformación Digital, sin embargo, esta se ve limitada como instancia de coordinación exclusiva y vinculante para asuntos de Seguridad Digital.
Confianza	Si bien se han desarrollado nexos con participación entre entidades públicas y privadas en casos particulares (Ej. CSIRTs sectoriales, operadores y propietarios de Infraestructuras Críticas, entre otros), la baja articulación con otras partes interesadas limita la generación de confianza entre éstas.
Gestión de riesgos con visión integral	No obstante los esfuerzos por disponer de un modelo nacional de gestión de riesgos, el mismo no es resultado de un consenso en relación con la visión que tienen otras partes interesadas. Existen partes interesadas que aún no hacen gestión de riesgos de seguridad digital.
Capacidades	No existen suficientes esfuerzos coordinados para cerrar brechas entre capacidades de seguridad digital de las distintas partes interesadas.
Orientación para el posicionamiento internacional	Existe un canal (Ministerio de Relaciones Exteriores) para las gestiones relacionadas con las posturas, adopción a artefactos e instrumentos internacionales. Sin embargo, persisten situaciones que limitan la articulación que debería existir para establecer posturas país, realizar debates y elevar la participación de Colombia en escenarios internacionales, como, por ejemplo, esfuerzos aislados en gestiones de cooperación y asistencia, y baja comprensión del contexto internacional de la Seguridad Digital, entre otras.
Participación de las múltiples partes interesadas	Se ha mejorado la interacción especialmente entre instancias de ciberseguridad y ciberdefensa del Gobierno. Se han generado interacciones con el sector privado, particularmente con equipos de respuesta a incidentes y con propietarios u operadores de infraestructuras críticas a través de las reuniones de Infraestructura Crítica Cibernética, Riesgo Operacional y Ciberdefensa. Sin embargo, el diálogo con otras partes interesadas aún es muy limitado.
Recursos orientados a dinamización de la interacción	No se cuenta con recursos suficientes para adelantar acciones que promuevan estrategias y acciones inherentes para impulsar la coordinación, colaboración, cooperación y asistencia entre las partes interesadas.
Mecanismos de interacción	Existen propuestas y desarrollos iniciales de mecanismos para facilitar la coordinación, colaboración, cooperación y asistencia en aspectos relacionados con seguridad digital, sin embargo, los mismos son insuficientes para generar el diálogo y empoderamiento.
Escenarios de discusión de propuestas	Los entornos y mecanismos de colaboración no resultan suficientes para permitir la participación efectiva de las partes en generación y discusión de propuestas sobre políticas, mejores prácticas, modelos y adopción de estándares asociados a la seguridad digital.
Conocimiento y talento especializado	Se han logrado avances en la generación de talento especializado para algunas de las partes, sin embargo, persisten brechas en actores con pocas capacidades, así como pocos escenarios en los que se comparta el conocimiento en esta materia.

Según el Foro Económico Mundial, la falta de un marco de gobernanza global para la tecnología corre el riesgo de fragmentar el ciberespacio, lo que podría disuadir el crecimiento económico, agravar las rivalidades geopolíticas y ampliar las divisiones dentro de las sociedades, por lo tanto es urgente una arquitectura de gobernanza global más completa, inclusiva y ágil para abordar los problemas de seguridad dinámicos e interrelacionados que plantea la Cuarta Revolución Industrial (WEF, 2020)

A nivel internacional, como lo evaluó la OEA, el análisis de las buenas prácticas indica que para la formulación de un modelo de gobernanza es indispensable revisar al menos los siguientes aspectos: i) el enfoque, ii) la definición, iii) los principios orientadores, iv) los objetivos específicos y las macroactividades, v) los tipos de interacción entre las partes, y vi) los tipos de alianzas entre las partes. Estos elementos fueron debidamente considerados en desarrollo del producto "Modelo de Gobernanza para mejorar la Seguridad Digital en Colombia", el cual fue entregado por la OEA al Ministerio de Tecnologías de la Información y las Comunicaciones en el marco del Convenio precitado y el cual fue desarrollado con participación no solo de los consultores expertos de la OEA, sino que contó con aportes obtenidos en espacios de trabajo en los que aportaron las diferentes partes interesadas en Seguridad Digital en Colombia, por lo que resulta un ejercicio que además de incorporar las mejores prácticas internacionales en la materia, responde a las necesidades y características particulares del país, constituyéndose en un insumo fundamental para la gestión de la seguridad digital en Colombia.

Por lo indicado, es indispensable que los países cuenten con modelos de gobernanza claros en asuntos que tienen relación con el acceso, adopción, gestión y uso de tecnología que contribuyan a este marco de gobernanza global, siendo uno de estos asuntos la seguridad digital. Según la *Guía para la Elaboración de una Estrategia Nacional de Ciberseguridad* de la Unión Internacional de Telecomunicaciones -UIT-[1], el establecimiento de un modelo de gobernanza de seguridad digital es una práctica prioritaria que cada país debe diseñar y adaptar a su contexto nacional y que puede mejorar la integridad y eficacia de las políticas nacionales en torno al tema.

Es así como se plantea adoptar un Modelo de Gobernanza de Seguridad Digital para Colombia, como un modelo de articulación y armonización de las múltiples partes interesadas con el fin de fortalecer las capacidades para la gestión de riesgos e incidentes de seguridad digital y para la respuesta proactiva y reactiva a posibles amenazas a la confidencialidad, integridad o disponibilidad de las computadoras, redes e información que en conjunto constituyen el entorno digital en el país. La gobernanza de la seguridad digital para Colombia se refiere a los enfoques utilizados por múltiples partes interesadas para identificar, enmarcar y coordinar respuestas proactivas y reactivas a posibles amenazas a la confidencialidad, integridad o disponibilidad de las computadoras, redes e información que en conjunto constituyen el entorno digital.

El *Modelo de Gobernanza de Seguridad Digital de Colombia* que se pretende adoptar tiene las siguientes características:

- Es modular y flexible para permitir que los programas y proyectos se adapten a las necesidades y a los diferentes actores, asegurando un enfoque específico de la creación de capacidad.
- Es complementario para minimizar la duplicación de esfuerzos y beneficiarse de una coordinación bien organizada.
- Es multinacional para incluir a todos las instancias y autoridades de gobierno: nacional, territorial y local.
- Es multinivel integrando asuntos en los siguientes niveles:
    - Nivel Estratégico: procesos para generar productos de dirección y orientación estratégica y tomar decisiones sobre la asignación eficiente de recursos escasos
    - Nivel Táctico: procesos para generar productos derivados de la interacción eficiente entre las partes para lograr objetivos comunes

[1] La guía fue elaborada por doce asociados de organizaciones intergubernamentales e internacionales, del sector privado, así como del mundo académico y de la sociedad civil, concretamente las siguientes: la Secretaría del Commonwealth (COMSEC), Organización de Telecomunicaciones del Commonwealth (CTO), DELOITTE, Centro de Política de Seguridad de Ginebra (GCSP), Centro Global de Capacitación en Ciberseguridad (GCSCC) de la Universidad de Oxford, Unión Internacional de Telecomunicaciones (UIT), MICROSOFT, Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE OTAN), Instituto Potomac de Estudios Políticos, RAND Europa, Banco Mundial y Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD). También aportó la Agencia Europea de Seguridad de las Redes y de la Información (ENISA).

- Nivel Operacional: procesos para generar productos derivados del cumplimiento de actividades y acciones puntuales
- Es multisectorial para que las múltiples partes interesadas de todos los sectores aporten capacidades y recursos desde sus roles específicos
- Es multidisciplinario para permitir el análisis de los problemas y temáticas objeto de análisis teniendo en cuenta todas las disciplinas y ámbitos, así como las visiones desde diferentes ópticas (técnico, económico, jurídico, social, etc.)

Adicionalmente, el *Modelo de Gobernanza de Seguridad Digital de Colombia* propenderá por maximizar:

- la efectividad, la eficacia, la eficiencia y la legitimación de los procesos de consulta y de toma de decisiones
- el uso de modelos flexibles que potencien las relaciones verticales y horizontales entre partes
- la asignación eficiente y compartida de recursos escasos
- la formulación e implementación de decisiones públicas mediante el uso efectivo de alianzas y redes de interacción
- la participación interactiva y simétrica entre las partes
- la adaptabilidad a medida que cambian los problemas y se pueden aprender de manera innovadora nuevas respuestas a los mismos

De igual manera, el *Modelo de Gobernanza de Seguridad Digital de Colombia* propenderá por minimizar:

- el uso de estructuras de consulta demasiado complejas o extremadamente formales
- los costos de transacción derivados de la interacción entre las partes
- el riesgo de deslegitimación fomentando la interacción decisional entre las partes
- el riesgo de inefectividad de las decisiones asegurando claridad previa de los intereses y necesidades de las partes

Así las cosas, se justifica emitir los lineamientos correspondientes para que el país pueda adoptar el modelo de Gobernanza de Seguridad aquí señalado.

Por lo anterior, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital, se expiden las presentes disposiciones.

2. En materia de gestión de riesgos e incidentes de seguridad digital:

Es necesario fortalecer las capacidades para gestionar adecuadamente los riesgos de seguridad digital de las entidades públicas del país ya que de acuerdo con las últimas mediciones realizadas en Colombia al respecto expuestas en el estudio del estado de la Ciberseguridad en las Organizaciones Colombianas 2018-2019 (Ministerio de Tecnologías de la Información y las Comunicaciones, BID, OEA, 2019) establece que en el 58% de las organizaciones públicas no existe área con funciones asignadas a la seguridad digital. Esto además de mostrar que no existen las capacidades de gestión respecto a seguridad digital al interior de las entidades, propicia que no se priorice la vinculación de profesionales con este tipo de formación pues no se tiene justificación suficiente para hacer la vinculación de personal en la misma.

Frente a las capacidades de gestión de riesgos de seguridad digital, el estudio antes mencionado también encuentra que existen falta de apoyo del nivel directivo de las organizaciones públicas. El estudio establece que la principal razón para la disminución del presupuesto de seguridad digital en las organizaciones públicas participantes fue precisamente la falta de concientización del nivel directivo en lo relacionado en seguridad digital, ya que el 57% de las entidades señalaron esta motivación.

Igualmente, las prácticas en seguridad digital no son adoptadas adecuadamente en las organizaciones públicas, especialmente en el nivel territorial. En promedio el 43% de las organizaciones públicas colombianas participantes en el mismo estudio manifiestan que no adoptaron prácticas en gestión de riesgos de seguridad digital en 2018, evidenciándose un gran contraste según el tipo de entidad, mientras solo el 9% de las entidades del orden nacional afirma no haber adoptado este tipo de prácticas, el 46% de las entidades territoriales del orden departamental y el 54% de las del orden municipal reconocen incurrir en esta debilidad.

Todo lo anterior, afecta las capacidades de las organizaciones públicas respecto a la posibilidad de gestionar adecuadamente los riesgos de seguridad digital y es necesario expedir lineamientos y normatividad que establezca responsabilidades para las entidades públicas, respecto al reporte y gestión de riesgos e incidentes de seguridad digital que permita mejorar la protección de la información tratada en las entidades públicas del país.

3. En materia de identificación, catalogación, categorización e inventario de las infraestructuras criticas cibernéticas:

Desde el año 2016 se ha venido adelantando la ardua tarea de identificación, catalogación y priorización de las infraestructuras criticas cibernéticas nacionales (ICCN) de Colombia, con el fin de fijar una línea de ruta que le permita plantear de manera organizada y priorizada las directrices de seguridad aplicables en todos los sectores de infraestructura crítica; propendiendo por un enfoque prioritario, flexible, repetible, basado en estándares aceptados; lo que da lugar a identificar, evaluar y gestionar el riesgo cibernéticos; de cada uno de los (13) trece sectores, atendiendo a su línea de criticidad; este contexto y tiendo en cuenta lo fijado en la Metodología implementada en el Modelo Integrado de Capacidad de Madurez propuesto por Carnegie Mellon University, Software Engineering Institute, se encuentra realizando la actualización y retroalimentación del inventario de infraestructuras críticas según el sector y ámbito de protección estratégico, conociendo que esta es la base necesaria que permite dirigir y coordinar las actuaciones de las distintas entidades tanto públicas como privadas en materia de protección de infraestructuras, de lo anterior, se prevé la necesidad de una correcta identificación y designación de las mismas, para mejorar la prevención, preparación y respuesta de nuestro Estado frente a atentados terroristas u otras amenazas que afecten a infraestructuras críticas en materia cibernética .

De estas actuaciones parciales, es la razón por la cual un correcto inventario y categorización se hace importante y necesario al momento de conocer el estado del arte del ecosistema digital en materia de infraestructura. Teniendo en cuenta, que la finalidad principal de la catalogación es valorar y gestionar los datos disponibles de las diferentes infraestructuras, con el objetivo de diseñar los mecanismos de planificación, prevención, protección y reacción ante una eventual amenaza y, en caso de ser necesario, activar, conforme a lo previsto en los planes de protección de las infraestructuras críticas, atender riesgos a las vulnerabilidades y amenazas potenciales.

En razón a lo anterior, y teniendo en cuenta que a la fecha se pueden identificar aproximadamente 2.800 infraestructuras, divididas en los 13 sectores con diferentes tecnologías y enfoques técnicos, se hace necesario impulsar, además, la colaboración e implicación de los propietarios de dichas infraestructuras, a fin de optimizar el grado de protección de éstas contra ataques deliberados de todo tipo, lo que permite contribuir a la protección de los servicios esenciales y aras de preservar la seguridad, defensa y el cumplimiento de los fines esenciales del Estado.

El objeto que se pretende adoptar en materia de las infraestructuras criticas cibernéticas tiene las siguientes características y alcances:

- Fijar la estandarización del Plan Nacional de Protección de Las Infraestructuras Críticas
- Regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales.
- Constituir un sistema de notificación de incidentes.
- Establecer los Planes estratégicos sectoriales
- Fundar los Planes de seguridad del operador según las tecnologías utilizadas por la infraestructura.
- Determinar los Planes de protección específicos
- Precisar los Planes de apoyo operativos.

Finalmente, y basados en lo anterior, el análisis y categorización sistematizado que se adelante, permitirá generar de manera focalizada la compartimentación de información frente a los riesgos conforme a su enfoque específico, tanto de carácter físico como lógico, de allí se podrá generar documentos estratégicos definidores de las políticas generales de los operadores críticos para garantizar la seguridad las infraestructuras según su grado de criticidad, de lo anterior dependerá la respuesta ágil, oportuna y proporcionada, de acuerdo con el nivel y características de la amenaza el poder contenerla y adoptar las medidas de resiliencia requeridas.

Por ello, se hace necesario establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital

b) AMBITO DE APLICACIÓN Y SUJETOS A QUIENES VA DIRIGIDO

Serán sujetos obligados las entidades que conforman la Administración Pública en los términos del artículo 39 de la Ley 489 de 1998 y los particulares que cumplen funciones públicas o administrativas y a las múltiples partes interesadas del ecosistema digital que en el marco de sus competencias y responsabilidades, deban garantizar o contribuir a la seguridad digital, la protección de las redes, las infraestructuras críticas, los servicios esenciales y los sistemas de información en el ciberespacio.

La implementación del presente decreto en las Ramas Legislativa y Judicial, en los órganos de control, en los autónomos e independientes y demás organismos del Estado, se realizará bajo un esquema de coordinación y colaboración armónica en aplicación de los principios señalados en los artículos 113 y 209 de la Constitución Política.

Las personas jurídicas de derecho privado que tengan a su cargo la prestación de servicios y que cuentan con infraestructuras críticas cibernéticas o presten servicios esenciales deberán adoptar medidas técnicas, humanas y administrativas para garantizar la gobernanza de la seguridad digital, la gestión de riesgos, la identificación y reporte de infraestructuras críticas y servicios esenciales, y la respuesta a incidentes de Seguridad Digital.

3. VIABILIDAD JURÍDICA

(Por favor desarrolle cada uno de los siguientes puntos)

3.1 Análisis de las normas que otorgan la competencia para la expedición del proyecto normativo

En virtud del numeral 2 del artículo 17 de la Ley 1341 de 2009, el Ministerio de Tecnologías de la Información y las Comunicaciones tiene entre sus objetivos "(…) 2. Promover el uso y apropiación de las Tecnologías de la Información y las Comunicaciones entre los ciudadanos, las empresas, el Gobierno y demás instancias nacionales como soporte del desarrollo social, económico y político de la Nación"

La Ley 1437 de 2011, "Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo", a través de su artículo 64 faculta al Gobierno Nacional para definir los estándares y protocolos que deberán cumplir las autoridades para incorporar en forma gradual los medios electrónicos en los procedimientos administrativos, entre los que se cuentan los relativos a la seguridad digital.

A través del Documento Conpes 3701 del 14 de julio de 2011, por medio del cual se dieron lineamientos de política para Ciberseguridad y Ciberdefensa, se implementaron instancias para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional. Uno de sus objetivos específicos es, conformar organismos con la capacidad técnica y operativa necesaria para la defensa y seguridad nacional en materia cibernética.

De acuerdo con el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015, "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones", la Política de Gobierno Digital será definida por el Ministerio de Tecnologías de la Información y las Comunicaciones y se desarrollará a través de componentes y habilitadores transversales que, acompañados de lineamientos y estándares, permitirán el logro de propósitos que generarán valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC.

Según el mismo artículo 2.2.9.1.2.1, los habilitadores transversales de la Política de Gobierno Digital, son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los componentes y el logro de los propósitos de dicha Política.

De acuerdo con el numeral 12 del artículo 2.2.22.2.1. del Decreto 1083 de 2015, "Decreto Único Reglamentario del Sector Función Pública", la política de Seguridad Digital forma parte de las políticas de Gestión y Desempeño Institucional. Así mismo, el numeral 5 del artículo 2.2.22.3.6. define como una de las funciones de los Comités Sectoriales de Gestión y Desempeño "Dirigir y articular a las entidades del sector administrativo en la operación de las políticas de gestión y desempeño y de las directrices impartidas por la Presidencia de la República y el Ministerio de Tecnologías de la Información y las Comunicaciones en materia de Gobierno y Seguridad Digital".

De acuerdo con el numeral 5 del artículo 2.2.22.3.7. del citado Decreto 1083 de 2015, una de las funciones de los Comités Departamentales, Distritales y Municipales de Gestión y Desempeño "Dirigir y articular a las entidades del departamento, distrito o municipio en la implementación y operación de las políticas de gestión y desempeño y de las directrices impartidas por la Presidencia de la República y el Ministerio de Tecnologías de la Información y las Comunicaciones en materia de Gobierno y Seguridad Digital". Por su parte, el numeral 6 del artículo 2.2.22.3.8, define como una de las funciones de los Comités Institucionales de Gestión y Desempeño "Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información".

El Conpes 3854 del 11 de abril de 2016, establece la Política Nacional de Seguridad Digital, mediante la cual crea las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital, siendo uno de los principales aportes de esta política el desarrollo de estrategias que establecieron un marco institucional para la seguridad digital con un enfoque de gestión de riesgos, es decir, con una visión preventiva antes que reactiva ante las posibles amenazas en seguridad digital. Mediante la política precitada se generaron mecanismos estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad digital a nivel nacional e internacional y se creó la figura de Coordinador Nacional de Seguridad Digital, la cual se encuentra actualmente en cabeza de la Consejería Presidencial de Asuntos Económicos y Transformación Digital de la Presidencia de la República.

El artículo 147 de la Ley 1955 de 2019 "Por la cual se expide el Plan Nacional de Desarrollo 2018-2022 "pacto por Colombia, pacto por la equidad" señala la obligación de las entidades estatales del orden nacional, de incorporar en sus respectivos planes de acción el componente de transformación digital, siguiendo los estándares que para este propósito defina el Ministerio de Tecnologías de la Información y las Comunicaciones. De acuerdo con el mismo precepto, los proyectos estratégicos de transformación digital se orientarán entre otros, por la aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.

El artículo 230 de la Ley 1450 de 2011, modificado por el artículo 148 de la Ley 1955 de 2019 señala que "Todas las entidades de la administración pública deberán adelantar las acciones que señale el Gobierno nacional a través del Ministerio de Tecnologías de la Información y las Comunicaciones para la implementación de la política de Gobierno Digital". Dentro de las acciones prioritarias se encuentran el cumplimiento de los lineamientos y estándares para el incremento de la confianza y la seguridad digital.

El Conpes 3995 de 2020, Política Nacional de Confianza y Seguridad Digital, señala como un objetivo establecer medidas para desarrollar la confianza digital a través de la mejora en la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

Que, con fundamento en lo anterior, se hace necesario disponer de un marco para la gobernanza de la seguridad digital del país, así como implementar y aplicar Modelos de Gestión de Riesgos de Seguridad y un Modelo Nacional de Atención a Incidentes y la creación de un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT GOBIERNO) por sus siglas en inglés (Computer Security Incident & Response Team), con el fin de prevenir y mitigar los riesgos de seguridad y generar confianza.

3.2 Vigencia de la ley o norma reglamentada o desarrollada

Las disposiciones contenidas en el numeral 11 del artículo 189 de la Constitución Política, el artículo 64 de la Ley 1437 de 2011 y los artículos 147 de la Ley 1955 de 2019 y 230 de la Ley 1450 de 2011, modificado por el artículo 148 de la Ley 1955 de 2019, se encuentran vigentes.

3.3. Disposiciones derogadas, subrogadas, modificadas, adicionadas o sustituidas

El proyecto normativo adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital

3.4 **Revisión y análisis de la jurisprudencia que tenga impacto o sea relevante para la expedición del proyecto normativo (órganos de cierre de cada jurisdicción)**

No existen decisiones judiciales de los órganos de cierre de cada jurisdicción que puedan tener impacto o ser relevantes para la expedición del acto administrativo.

3.5 **Circunstancias jurídicas adicionales**

No existe ninguna otra circunstancia jurídica que deba ser atendida al ser relevante para la expedición del acto.

4. IMPACTO ECONÓMICO (Si se requiere)
(Por favor señale el costo o ahorro de la implementación del acto administrativo)

La expedición del proyecto por el cual se se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital no representa una erogación económica adicional a la que vienen haciendo las autoridades para garantizar la seguridad digital.

5. VIABILIDAD O DISPONIBILIDAD PRESUPUESTAL (Si se requiere)
(Por favor indique si cuenta con los recursos presupuestales disponibles para la implementación del proyecto normativo)

El proyecto de decreto no representa nuevas disponibilidades presupuestales a las ya dispuestas en el marco de la política de gobierno digital.

6. IMPACTO MEDIOAMBIENTAL O SOBRE EL PATRIMONIO CULTURAL DE LA NACIÓN (Si se requiere)
(Por favor indique el proyecto normativo tiene impacto sobre el medio ambiente o el Patrimonio cultural de la Nación)

El proyecto normativo bajo análisis no tendrá impacto sobre el medio ambiente, como tampoco sobre el patrimonio cultural de la Nación.

7. ESTUDIOS TÉCNICOS QUE SUSTENTEN EL PROYECTO NORMATIVO (Si cuenta con ellos)

Metodología de plazos para la digitalización y automatización de trámites – Anexo a la memoria justificativa del proyecto
Anexo técnico para la digitalización y automatización de trámites.

ANEXOS:	
Certificación de cumplimiento de requisitos de consulta, publicidad y de incorporación en la agenda regulatoria *(Firmada por el servidor público competente –autoridad originadora)*	*X*
Concepto(s) de Ministerio de Comercio, Industria y Turismo *(Cuando se trate de un proyecto de reglamento técnico o de procedimientos de evaluación de conformidad)*	*(Marque con una x)*
Informe de observaciones y respuestas *(Análisis del informe con la evaluación de las observaciones de los ciudadanos y grupos de interés sobre el proyecto normativo)*	*X*
Concepto de Abogacía de la Competencia de la Superintendencia de Industria y Comercio *(Cuando los proyectos normativos tengan incidencia en la libre competencia de los mercados)*	*(Marque con una x)*
Concepto de aprobación nuevos trámites del Departamento Administrativo de la Función Pública *(Cuando el proyecto normativo adopte o modifique un trámite)*	*(Marque con una x)*
Otro *(Cualquier otro aspecto que la autoridad originadora de la norma considere relevante o de importancia)*	*(Marque con una x)*

Aprobó:

INGRID TATIANA MONTELAGRE
Directora de Gobierno Digital

SIMON RODRIGUEZ SERNA
Director Jurídico

Elaboró: Marco Emilio Sánchez Acevedo Abogado Equipo de Política Dirección de Gobierno Digital
Diego Bohórquez – Departamento Admiisntastivo del a Presiedncia de la República
Jorge Bejarano – Departamento Admiisntastivo del a Presiedncia de la República
Angela Cortés – Dirección de Gobierno Digital
Danny Alejandro Garzón Aristizabal - Dirección de Gobierno Digital

Revisó:

Ingrid Tatiana Montealegre – Directora de Gobierno Digital
Margarita Ricardo - Asesor Despacho Viceministerio de Transformación Digital

Luis Leonardo Monguí Rojas – Coordinador GIT de Doctrina y Seguridad Jurídica

Aprobó: Ivan Durán – Viceministro de Transformación Digital