REPUBLICA DE COLOMBIA

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

DECRETO N° DE

"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 cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital"

EL PRESIDENTE DE LA REPÚBLICA DE COLOMBIA

En ejercicio de sus facultades constitucionales y legales, en especial las que le confiere 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,

CONSIDERANDO

Que, conforme al principio de "masificación del gobierno en línea" hoy Gobierno Digital, consagrado en el numeral 8 del artículo 2 de la Ley 1341 de 2009 "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC– ,(…)", "(…) las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones (…)"

Que, 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"

Que, 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.

Que, 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.

Que, 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.

Que, 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.

Que, 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".

Que, 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".

Que, 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.

"

"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 cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital"

Que, 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.

Que, 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.

Que, 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.

Que, con el objetivo de generar un proceso continuo de gestión de riesgos adaptable a nuevas tecnologías actuales y futuras, las autoridades deben contemplar temas referentes a tecnologías emergentes, cibercultura, resiliencia y seguridad en el ecosistema, que les permitan operar de una manera segura y generando confianza en los servicios ciudadanos ofrecidos.

Que, el Ministerio de Tecnologías de la Información y las Comunicaciones ha establecido de igual forma un Modelo de Seguridad y Privacidad de la Información – MSPI, el cual conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

Que, 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

"

"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 cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital"

Incident & Response Team), con el fin de prevenir y mitigar los riesgos de seguridad y generar confianza.

Que, en cumplimiento de los artículos 3 y 8 la Ley 1437 de 2011 y 2.1.2.1.14 del Decreto 1081 de 2015, "Decreto Reglamentario Único del Sector Presidencia de la República", las disposiciones del presente proyecto de decreto fueron publicadas en la sede electrónica del Ministerio de Tecnologías de la Información y las Comunicaciones, durante el periodo comprendido entre el 1 de febrero de 2022 y el 15 de febrero de 2022.

En mérito de lo expuesto,

DECRETA

ARTÍCULO 1. Adiciónese 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, el cual quedará así:

"TÍTULO 21

"LINEAMIENTOS GENERALES PARA FORTALECER LA GOBERNANZA DE LA SEGURIDAD DIGITAL, LA IDENTIFICACIÓN DE INFRAESTRUCTURAS CRÍTICAS CIBERNÉTICAS Y SERVICIOS ESENCIALES, LA GESTIÓN DE RIESGOS Y LA RESPUESTA A INCIDENTES DE SEGURIDAD DIGITAL"

CAPÍTULO 1

LINEAMIENTOS GENERALES

SECCIÓN 1

OBJETO, ÁMBITO DE APLICACIÓN, DEFINICIONES, LINEAMIENTOS GENERALES Y PRINCIPIOS

ARTÍCULO 2.2.21.1.1.1. *Objeto*. El presente título tiene por objeto reglamentar parcialmente los artículos 147 y 230 de la Ley 1450 de 2011, modificado por el artículo 148 de la Ley 1955 de 2019 y el artículo 64 de la Ley 1437 de 2011, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital.

ARTÍCULO 2.2.21.1.1.2. *Ámbito de aplicación.* Los sujetos obligados de las disposiciones contenidas en el presente título serán 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 cibernéticas y su entorno, los servicios esenciales y los sistemas de información en el ciberespacio.

"

"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 cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital"

Parágrafo 1. 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.

Parágrafo 2. Las personas jurídicas de derecho privado que tengan a su cargo la prestación de servicios y que administren y gestionen 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 cibernéticas y servicios esenciales, y la respuesta a incidentes de Seguridad Digital.

Artículo 2.2.21.1.1.3. *Definiciones*. Para efectos de lo establecido en este título, se tendrán en cuenta las siguientes definiciones:

1. **CERT: (**Computer Emergency Response Team) Equipo de Respuesta a Emergencias cibernéticas. Se refiere a una institución definida y concreta con capacidad centralizada para la coordinación de gestión de incidentes.

2. **Ciberespacio:** Entorno virtual complejo resultante de la interacción de personas, software, hardware y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red.

3. **CSIRT: (**Computer Security Incident & Response Team**)** Equipo de Respuesta a Incidentes de Seguridad Cibernética, por su sigla en inglés. Se refiere a una institución definida y concreta que tiene la responsabilidad de proveer capacidades de gestión de incidentes a una organización/sector en especial. Su objetivo es minimizar y controlar el daño resultante de incidentes, proveyendo la respuesta, contención y recuperación efectiva, así como trabajar en pro de prevenir la ocurrencia de futuros incidentes.

4. **CSIRT sectorial:** Son los equipos de respuesta a incidentes sectoriales de cada uno de los sectores identificados en el ecosistema digita.

5. **CSIRT sectorial crítico:** Son los equipos de respuesta a incidentes sectoriales de cada uno de los sectores identificados como críticos.

6. **Gobernanza de la seguridad digital para Colombia:** Se refiere a los enfoques utilizados por múltiples partes interesadas para identificar, enmarcar, proponer, y coordinar respuestas proactivas y reactivas a posibles amenazas a la confidencialidad, integridad o disponibilidad de los servicios tecnológicos, sistemas de información, infraestructura tecnológica,, redes e información que en conjunto constituyen el entorno digital.

7. **Incidente de seguridad digital:** cualquier evento adverso intencionado o no intencionado, que puede cambiar o afectar el curso esperado de una actividad en el entorno digital.

"

8. **Infraestructura crítica cibernética:** Son las infraestructuras estratégicas soportadas por Tecnologías de la Información y las Comunicaciones (TIC) o Tecnologías de Operación (TO), cuyo funcionamiento es indispensable, por lo que su suspensión, afectación, o destrucción tendría un grave impacto o efecto perturbador sobre los servicios esenciales del Estado.

9. **Infraestructura estratégica:** Son las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que se soporta el funcionamiento de los servicios esenciales.

10. **Modelo de Gobernanza de Seguridad Digital:** Se define 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 los servicios tecnológicos, sistemas de información, infraestructura tecnológica y las redes e información que en conjunto constituyen el entorno digital en el país

11. **Múltiples partes interesadas:** Se refiere a los distintos actores que tienen interés en los aspectos relacionados con la Seguridad Digital en Colombia.

12. **Operador de servicios esenciales establecido en Colombia**: Es la persona jurídica, pública o privada, que presta un servicio esencial y cuenta con una residencia o domicilio social en territorio Nacional, siempre que estos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios o actividades. Así mismo, esta definición se aplicará a los servicios esenciales que los operadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en territorio nacional. También serán operadores de servicios esenciales establecidos en Colombia, los Proveedores de Redes y Servicios de Telecomunicaciones (PSRT) que tengan su sede social acorde con la legislación colombiana y que constituya su actividad de negocio relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en el territorio nacional.

13. **Seguridad de la información:** Preservación de la autenticidad, confidencialidad, integridad, y disponibilidad de la información de las partes interesadas en cualquier medio de almacenamiento: impreso o digital, y la aplicación de procesos de resiliencia operativa.

14. **Seguridad digital:** Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), a través de la apropiación de políticas y buenas prácticas y mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas.

15. **Servicio esencial:** Es el servicio necesario para el mantenimiento de las actividades sociales y económicas del país, que dependen del uso de tecnologías de la información y las comunicaciones, y un incidente en su

infraestructura o servicio podría generar un daño significativo que afecte la prestación de dicho servicio y la consecuente parálisis de las actividades.

16. **Vulnerabilidad de seguridad digital**: Debilidad, atributo o falta de aplicación de un control que permite o facilita la actuación de una amenaza contra los servicios tecnológicos, sistemas de información, infraestructura tecnológica y las redes e información de la organización.

ARTÍCULO 2.2.21.1.1.4. *Lineamientos generales*. Los sujetos obligados deberán adoptar medidas técnicas, humanas y administrativas para garantizar la gobernanza de la seguridad digital, la gestión de riesgos de Seguridad Digital, la identificación y reporte de infraestructuras críticas cibernéticas y servicios esenciales, y la respuesta a incidentes de seguridad digital.

ARTÍCULO 2.2.21.1.1.5. *Principios.* Además de los principios previstos en los artículos 209 de la Constitución Política, 2° de la Ley 1341 de 2009, 3° de la Ley 1437 de 2011, 4° de la Ley 1581 de 2012 y los atinentes a la Política de Gobierno Digital contenidos en el artículo 2.2.9.1.1.3 del Decreto 1078 de 2015, a los efectos del presente decreto se aplicarán los siguientes:

1. **Confianza**. La seguridad digital debe fomentar la confianza mediante la buena comunicación, el intercambio de información y la concreción de acuerdos claros sobre la división de tareas y acciones a realizar.

2. **Coordinación.** Las actuaciones que se realicen en materia de seguridad digital a través del ciberespacio, deberán integrar de manera coordinada a las múltiples partes interesadas, para garantizar la armonía en el ejercicio de sus funciones y el logro del objeto del presente título.

3. **Colaboración entre las múltiples partes interesadas**. En la aplicación e interpretación de los presentes lineamientos se deben involucrar activamente a las múltiples partes interesadas, y permitir establecer condiciones para el desarrollo eficiente de alianzas, con el fin de promover la seguridad digital del país y sus habitantes, y aumentar la capacidad de resiliencia nacional frente a eventos no deseados en el entorno digital y con ello fomentar la prosperidad económica y social, buscando la generación de riqueza, innovación, productividad, competitividad, y empleo en todos los sectores de la economía.

4. **Cooperación.** En el marco de las relaciones nacionales e internacionales en materia de seguridad digital a través del ciberespacio, los sujetos obligados aunarán esfuerzos para el logro de los objetivos institucionales o comunes.

5. **Enfoque basado en la gestión de riesgos.** Los sujetos obligados deben gestionar el riesgo de forma que el uso de tecnologías de la información y las comunicaciones fomente la confianza en el entorno digital, la prosperidad económica y social, genere riqueza, innovación, productividad, competitividad, y empleo en todos los sectores de la economía, y ello no suponga la materialización de infracciones a los derechos de los ciudadanos.

"

6. **Gradualidad**. El Estado desarrollará, a través de las entidades y organismos competentes, las herramientas estratégicas y operativas, de alcance definido en tiempo, espacio y recursos presupuestales que permitan la implementación gradual y sostenida de estrategias, programas, planes y proyectos, que requiera el país para garantizar la seguridad, protección del ciberespacio.

7. **Inclusión.** La seguridad digital debe incluir a todas las partes interesadas, fomentar su participación activa y establecer condiciones necesarias para el desarrollo eficiente de alianzas.

8. **Proporcionalidad.** Las acciones y operaciones en el ciberespacio estarán en concordancia con la gestión dinámica de los riesgos derivados de los avances o usos de la ciencia y la tecnología, ponderando circunstancias de necesidad, derechos e intereses en juego, oportunidad, capacidades, amenazas y riesgos.

9. **Principio de enfoque incluyente y colaborativo.** Involucrar activamente a las múltiples partes interesadas, y permitir establecer condiciones para el desarrollo eficiente de alianzas, con el fin de promover la seguridad digital del país y sus habitantes, aumentar la capacidad de resiliencia nacional frente a eventos no deseados en el entorno digital y con ello fomentar la prosperidad económica y social, buscando la generación de riqueza, innovación, productividad, competitividad, y empleo en todos los sectores de la economía.

10. **Uso eficiente de la infraestructura y de los recursos para protección de las infraestructuras críticas cibernéticas y los servicios esenciales.** Los sujetos obligados velarán por las infraestructuras y los recursos tendientes a la protección de las infraestructuras críticas cibernéticas y los servicios esenciales para que sean aprovechados de forma eficiente y en beneficio de los derechos de los ciudadanos en el ciberespacio.

11. **Salvaguarda de los derechos humanos y los valores fundamentales de los ciudadanos.** En la aplicación e interpretación de los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la gestión de riesgos de Seguridad Digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, y la respuesta a incidentes de Seguridad Digital del sector gobierno de Colombia, se respetarán los derechos humanos y valores fundamentales incorporados en la Constitución Política y los tratados internacionales ratificados por Colombia.

SECCIÓN 2
Modelo de Gobernanza de Seguridad Digital

ARTÍCULO 2.2.21.1.2.1. ***Modelo de Gobernanza de la Seguridad Digital.*** Créase, el Modelo de Gobernanza de Seguridad Digital, de protección de las redes, las infraestructuras críticas cibernéticas, los servicios esenciales y los sistemas de información en el ciberespacio, quien tendrá a su cargo, entre otras, formular y ejecutar articuladamente las políticas, principios, objetivos y estrategias

"

"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 cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital"

dirigidas al fortalecimiento de la seguridad digital, de protección de las redes, las infraestructuras críticas, los servicios esenciales y los sistemas de información en el ciberespacio.

Los sujetos obligados acogerán el modelo de gobernanza descrito en el presente título y, desde sus competencias, aplicarán los objetivos, principios, niveles e instancias, que permitan su materialización.

ARTÍCULO 2.2.21.1.2.2. *Objetivos del Modelo de Gobernanza*: El Modelo de Gobernanza tiene como objetivo facilitar la participación, articulación e interacción de las múltiples partes interesadas para fortalecer las capacidades en la gestión de riesgos de seguridad digital y de esta manera lograr un abordaje integral que promueva el adecuado aprovechamiento de las oportunidades que ofrece el entorno digital.

Los objetivos específicos del Modelo de Gobernanza de Seguridad Digital son los siguientes:

1. Fortalecer el liderazgo y orientación estratégica de la seguridad digital del país con un enfoque participativo y colaborativo

2. Impulsar un enfoque holístico para la gestión de riesgos de Seguridad Digital

3. Proveer mecanismos para coordinar la gestión y respuesta a incidentes de seguridad digital

4. Promover la confianza para el intercambio de información y la gestión del conocimiento sobre seguridad digital en el país

5. Impulsar la generación de capacidades de seguridad digital de las partes interesadas de manera eficiente y colaborativa

ARTÍCULO 2.2.21.1.2.3. *Niveles del Modelo de Gobernanza:* Los niveles que enmarcan las acciones para la implementación de la Gobernanza de Seguridad Digital en el país, son los siguientes:

1. **Nivel estratégico:** Es el nivel en el que se definen las políticas y las prioridades estratégicas de la estrategia nacional. Determina los objetivos a largo plazo y el modo en que las múltiples partes interesadas han de interactuar entre sí.

2. **Nivel táctico:** Es el nivel en el que se elaboran los planes, procesos y procedimientos para coordinar las actividades de seguridad digital. Efectúa el control de la gestión realizada por el nivel operacional y soporta las decisiones que se toman y que afectan a las múltiples partes interesadas.

3. **Nivel operacional:** Es el nivel en el que se implementan y llevan a cabo actividades y tareas rutinarias definidas por el nivel táctico.

SECCIÓN 3

"

"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 cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital"

INSTANCIAS DEL MODELO DE GOBERNANZA DE LA SEGURIDAD DIGITAL

ARTÍCULO 2.2.21.1.3.1. ***Instancias de decisión del Modelo de Gobernanza:*** El modelo de Gobernanza de Seguridad Digital se implementará a partir de las siguientes instancias:

1. Comité Nacional de Seguridad Digital.
2. Coordinación Nacional de Seguridad Digital.
3. Grupos de Trabajo de Seguridad Digital
4. Las Mesas de Trabajo de Seguridad Digital.
5. Puestos de Mando Unificado de Seguridad Digital.

ARTÍCULO 2.2.21.1.3.2. ***Comité Nacional de Seguridad Digital:*** Créase el Comité Nacional de Seguridad Digital como una instancia de coordinación interinstitucional que tendrá como propósito impulsar la política de seguridad digital del país, y la orientación de acciones tendientes a fortalecer y promover un entorno digital confiable y seguro en el ciberespacio.

ARTÍCULO 2.2.21.1.3.3. Conformación del Comité Nacional de Seguridad Digital. El Comité Nacional de Seguridad Digital estará conformado por:

1. El Coordinador Nacional de seguridad digital o su delegado, quien presidirá el comité.
2. El Ministro de Hacienda y Crédito Público o su delegado.
3. El Ministro de Tecnologías de la Información y las Comunicaciones o su delegado.
4. El Ministro de Justicia y del Derecho o su delegado.
5. El Director del Departamento Nacional de Planeación o su delegado.
6. El Ministro de Cultura o su delegado.
7. El Ministerio de Relaciones Exteriores o su delegado.
8. El Ministerio de Defensa Nacional o su delegado.
9. El Comandante General de las Fuerzas Militares o su delegado.
10. El Director General de la Policía Nacional o su delegado.
11. El Director de la Dirección Nacional de Inteligencia o su delegado.
12. El Ministro de Educación Nacional o su delegado.
13. El Director de la Comisión de Regulación de Comunicaciones o su delegado
14. Un representante de cada uno de los sectores catalogados como titulares de infraestructura crítica cibernética o de servicios esenciales.

Al Comité Nacional de Seguridad Digitalasistirán, con voz pero sin voto las siguientes entidades:

1. El Fiscal General de la Nación o su delegado
2. El Procurador General de la Nación o su delegado

Parágrafo 1. Los delegados al Comité Nacional de Seguridad Digitaldeberán pertenecer a los niveles directivo o asesor que tengan a su cargo funciones relacionadas con políticas y estrategias en Seguridad Digital en la respectiva entidad.

"

"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 cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital"

Parágrafo 2. El Comité Nacional de Seguridad Digitalpodrá invitar a sus reuniones con carácter permanente u ocasional a otros expertos públicos o privados cuando los temas a tratar lo exijan.

ARTÍCULO 2.2.21.1.3.4. *Funciones del Comité Nacional de Seguridad Digital*: Son funciones del Comité Nacional de Seguridad Digital

1. Recomendar al alto gobierno, de oficio o a petición de parte, sobre todos los asuntos de política y las medidas estratégicas a nivel nacional con el fin de disuadir, detectar, prevenir, resistir, responder y recuperarse de acciones que comprometan o amenazan los sistemas informáticos, redes, infraestructuras, servicios digitales y la información de las organizaciones.
2. Apoyar la adecuada articulación y coordinación entre las entidades, autoridades y órganos, de todos los niveles, para facilitar la actuación, colaboración, comunicación y trabajo en equipo, con el fin de optimizar el ejercicio de sus competencias y funciones.
3. Proponer acciones que permitan fortalecer el desarrollo de las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital.
4. Presentar recomendaciones que sirvan de apoyo al proceso de toma de decisiones en materia de Seguridad Digital, defensa del ciberespacio, protección de las redes, las infraestructuras críticas cibernéticas, los servicios esenciales y los sistemas de información en el ciberespacio colombiano.
5. Articular el desarrollo de políticas y capacidades de seguridad digital para reducir el cibercrimen y el ciberdelito.
6. Darse su propio reglamento.
7. Evaluar y disponer la conformación de puestos de mando unificado ante eventos de seguridad digital.
8. Crear los grupos de trabajo necesarios para el cumplimiento de los fines señalados.
9. Las demás que sean señaladas en normas especiales.

ARTÍCULO 2.2.21.1.3.5. *Coordinación Nacional de Seguridad Digital:* El Presidente de la República designará al responsable de la Coordinación Nacional de Seguridad Digital que es la persona o dependencia responsable de coordinar los asuntos de seguridad digital en el Gobierno Nacional.

ARTÍCULO 2.2.21.1.3.6. *Funciones de la Coordinación Nacional de Seguridad Digital:* Son funciones de la Coordinación Nacional de Seguridad Digital:

1. Coordinar la implementación de políticas, iniciativas y programas estratégicos nacionales e internacionales de seguridad digital.
2. Identificar y desarrollar las prioridades e iniciativas de seguridad digital.
3. Coordinar esfuerzos para la convergencia de todas las actividades y programas de seguridad digital desarrollados o en implementación por las diferentes partes interesadas para someterlos a un monitoreo y evaluación constante.

"

4. Promover el desarrollo de alianzas y cooperación en materia de seguridad digital entre las múltiples partes interesadas.
5. Efectuar recomendaciones al Comité Nacional de Seguridad Digital con respecto a la priorización y asignación de recursos para mejorar la seguridad digital del país.
6. Apoyar el monitoreo y evaluación a la implementación de las políticas y estrategias nacionales de seguridad digital.

ARTÍCULO 2.2.21.1.3.7. *Grupos de Trabajo de Seguridad Digital:* Son grupos de personas conformados por representantes asignados de las múltiples partes interesadas, en los términos señalados por el Comité Nacional de Seguridad Digital.

Los grupos tienen la función de coordinar y asesorar al Comité Nacional de Seguridad Digital desde el punto de vista táctico y procedimental en torno a la seguridad digital a nivel nacional. Los grupos harán recomendaciones detalladas para fortalecer la seguridad digital, aumentar la confianza digital, mejorar las capacidades y mejorar la cooperación internacional.

El propósito de los grupos es apoyar la redacción de documentación técnica relevante y proporcionar información a la Coordinación Nacional de Seguridad Digital sobre el estado de los aspectos individuales de la implementación de las políticas y estrategias nacionales en las organizaciones y en la sociedad con base en los requerimientos de la Coordinación Nacional de Seguridad Digital.

ARTÍCULO 2.2.21.1.3.8. *Mesas de Trabajo de Seguridad Digital:* Son espacios técnicos especializados, definidos por los grupos de trabajo, en los se estudian y generan insumos a partir de la elaboración, ejecución, implementación y operación de los planes y/o documentación técnica requeridos en materia de Seguridad Digital.

ARTÍCULO 2.2.21.1.3.9. *Puestos de Mando Unificado de Seguridad Digital*. Instancia de colaboración y coordinación interinstitucional que tiene como objetivo articular y facilitar la toma de decisiones estratégicas y operaciones necesarias, para prevenir o gestionar incidentes cibernéticos sobre las infraestructuras críticas y los servicios esenciales, y que permiten la garantía de los derechos ciudadanos cuando actúan en el ciberespacio.

SECCIÓN 4
IDENTIFICACIÓN DE INFRAESTRUCTURAS CRÍTICAS CIBERNÉTICAS Y SERVICIOS ESENCIALES

ARTÍCULO 2.2.21.1.4.1. *Infraestructuras críticas cibernéticas y servicios esenciales*. Dentro de los doce (12) meses siguientes a la expedición del presente decreto, el Ministerio de Defensa Nacional, levantará el inventario de infraestructuras críticas cibernéticas nacionales y de servicios esenciales en el ciberespacio. Así mismo, realizará el inventario de los prestadores, operadores y responsables, que se encuentren establecidos o que operen en territorio colombiano. Dicho inventario se deberá actualizar como mínimo una vez cada año.

"

"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 cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital"

Para ello, deberá identificar los sectores y subsectores que cuentan con infraestructuras críticas cibernéticas o prestan servicios esenciales para el mantenimiento de las actividades económicas y sociales a partir de:

1. Que la entidad, pública o privada, desarrolle o preste una actividad o servicio fundamental para el mantenimiento de actividades sociales o económicas nacionales, o cuente con información privilegiada del nivel estratégico para el estado o la seguridad nacional.
2. La prestación de dicha actividad o servicio depende de las redes y sistemas de información, y/o de la utilización de Tecnologías de la Información y las Comunicaciones.
3. Un ataque o incidente en las redes y sistemas de información traería como consecuencia efectos significativos en la prestación de dicho servicio.

Parágrafo. El Ministerio de Defensa Nacional deberá señalar la metodología para realizar el levantamiento del inventario de infraestructuras críticas cibernéticas, de servicios esenciales, de operadores, prestadores y responsables de unos y otros, el régimen de obligaciones y el mecanismo de actualización de dichos registros. Esta metodología deberá incorporar mejores prácticas aplicables al levantamiento del inventario de Infraestructuras críticas cibernéticas, servicios esenciales e intereses nacionales para la Seguridad Digital.

ARTÍCULO 2.2.21.1.4.2. ***Vinculación de los sectores críticos y prestadores de servicios esenciales.*** Los sectores y subsectores que sean identificados como titulares de infraestructuras críticas cibernéticas o prestadores de servicios esenciales para el mantenimiento de las actividades económicas y sociales del país deberán vincularse como tales ante el Ministerio de Defensa Nacional -Comando Conjunto de Operaciones Cibernéticas - CCOCI.

El Ministerio de Defensa Nacional determinará, a más tardar el 1 de agosto de 2022, las condiciones de vinculación e integración para el desarrollo de las actividades señaladas en este decreto. Se deberá desarrollar como mínimo:

1. La supervisión al cumplimiento de las obligaciones por parte de los operadores de servicios esenciales y titulares de infraestructuras críticas cibernéticas.
2. Los canales de comunicación oportunos con los operadores o responsables de infraestructuras críticas cibernéticas y de servicios esenciales y con los proveedores de redes y servicios de telecomunicaciones (PRST).
3. Los sistemas de coordinación con los CSIRT sectoriales a través de los protocolos de actuación.
4. Procedimientos y canales para el reporte de infraestructuras críticas cibernéticas y prestadores de servicios esenciales.
5. Los puntos de contacto unificados.
6. El envío y recepción de las notificaciones sobre incidentes que sean presentadas en el marco de esta ley, a través de los CSIRT sectoriales.
7. La determinación de un punto de contacto único sobre las notificaciones de incidentes presentadas.
8. Los elementos e información que deben contener los incidentes reportados.

"

9. Las obligaciones específicas para garantizar la la Seguridad Digital, protección de las redes, de las infraestructuras, y los sistemas de información en el ciberespacio.
10. La delimitación de normas y especificaciones técnicas, para garantizar la Seguridad Digital, protección de las redes, de las infraestructuras, y los sistemas de información en el ciberespacio,
11. Las instancias de coordinación en los sectores y subsectores críticos y de servicios esenciales y su relación con los equipos de respuestas a incidentes.
12. Las cooperaciones internacionales en el marco de las obligaciones en cuanto a seguridad digital.

Parágrafo 1. Los sectores y subsectores que el Ministerio de Defensa Nacional defina como críticos, o aquellos que identifique, como prestadores de servicios esenciales para el mantenimiento y normal desarrollo de las actividades sociales y económicos de la nación propenderán por contar con un centro de respuesta a incidentes sectorial (CSIRT sectorial). El Ministerio de las Tecnologías de la Información y las Comunicaciones en coordinación con el Ministerio de Defensa Nacional, brindarán apoyo técnico y acompañamiento a la puesta en marcha de dichos equipos cuando les sea requerido.

ARTÍCULO 2.2.21.1.4.3. ***Obligaciones de seguridad de los titulares de infraestructura crítica, operadores de servicios esenciales.*** Las autoridades, públicas o privadas, definidos como críticos o prestadores de servicios esenciales, propenderán por contar con un plan de Seguridad Digital, protección de las redes, las infraestructuras críticas cibernéticas, los servicios esenciales y los sistemas de información en el ciberespacio y deberán hacer periódicamente una evaluación del riesgo de seguridad digital, que incluya una identificación de las mejoras a implementar en su Sistema de Administración del Riesgo Operativo. Para lo anterior, deben contar con normas, políticas, procedimientos, recursos técnicos, administrativos y humanos necesarios para gestionar efectivamente el riesgo, en los términos señalados en sus normas especiales y en cumplimiento de las mejores prácticas y estándares que le sean exigibles.

ARTÍCULO 2.2.21.1.4.4. ***Afectación significativa***. Para los efectos del presente Título, se entenderá por afectación significativa, aquella que se ocasiona a las Infraestructuras críticas cibernéticas, servicios esenciales e intereses nacionales para la Seguridad Digital, protección de las redes, de las infraestructuras, y los sistemas de información en el ciberespacio, y para determinarlo el Ministerio de Defensa Nacional tendrá en cuenta, entre otros, los siguientes factores:

1. El número de usuarios que confían en los servicios prestados por la entidad de que se trate;
2. La dependencia a otros sectores que se consideran críticos.
3. La repercusión que podrían tener los incidentes digitales, en términos de grado y duración, en las actividades económicas y sociales o en la seguridad pública;
4. La cuota de mercado que represente la entidad;
5. La extensión geográfica con respecto a la zona que podría verse afectada por un incidente digital;

6. La importancia de la entidad para mantener un nivel suficiente del servicio, teniendo en cuenta la disponibilidad de alternativas para la prestación de este.

SECCIÓN 5
MODELO NACIONAL DE ATENCIÓN Y GESTIÓN DE INCIDENTES.

ARTÍCULO 2.2.21.1.5.1. *Equipos de respuestas a incidentes de seguridad digital*: Para la atención y gestión de incidentes de seguridad digital el ColCERT - Grupo de Respuesta a Emergencias Cibernéticas de Colombia, el CSIRT – Gobierno – Grupo de Respuesta a Incidentes de Seguridad Digital de Gobierno, CSIRT – Defensa - Grupo de Respuesta a Incidentes de Seguridad Digital del sector Defensa, el CSIRT del Sector Inteligencia, , los CSIRT – Sectoriales - Grupos de Respuesta a Incidentes de Seguridad Digital de los sectores definidos como críticos o prestadores de servicios esenciales, atenderán las disposiciones señaladas en esta sección.

ARTÍCULO 2.2.21.1.5.2. *El ColCERT - Grupo de Respuesta a Emergencias Cibernéticas de Colombia*. El Ministerio de Tecnologías de la Información y las Comunicaciones coordinará el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) cuya finalidad es asesorar, apoyar y coordinar a las múltiples partes interesadas para la adecuada gestión de los riesgos e incidentes digitales. Así mismo, es el punto único de contacto y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel nacional e internacional de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Parágrafo 1. El Ministerio de Tecnologías de la Información y las Comunicaciones señalará las funciones que debe cumplir el ColCERT - Grupo de Respuesta a Emergencias Cibernéticas de Colombia.

Parágrafo 2. El lugar de operación, el talento humano y las herramientas del ColCERT será establecido y proporcionado por el Ministerio de Tecnologías de la Información y las Comunicaciones, anualmente.

ARTÍCULO 2.2.21.1.5.3. *Equipo de Respuesta a Incidentes de Seguridad cibernética para entidades del sector gobierno* (CSIRT GOBIERNO). El Ministerio de Tecnologías de la Información y las Comunicaciones coordinará el Equipo de Respuesta a Incidentes de Seguridad cibernética para entidades a que hace referencia el artículo 2.2.9.1.1.2. del Decreto, con el objetivo de prevenir y gestionar los incidentes de Seguridad Digital en el marco del modelo de seguridad y privacidad de la política de gobierno digital.

El lugar de operación, el talento humano y las herramientas de CSIRT Gobierno será establecido y proporcionado por el Ministerio de Tecnologías de la Información y las Comunicaciones, anualmente.

En los procesos estratégicos, misionales, de soporte y de mejora del CSIRT Gobierno, se deben adoptar y aplicar procedimientos, políticas, guías, protocolos, estándares, caracterizaciones y planes de acción que garanticen la adecuada

operación del CSIRT Gobierno, alineados al MSPI del Ministerio de TIC. Lo anterior con el objeto de generar un ecosistema seguro de intercambio de información técnica y de coordinación a nivel técnico, táctico y estratégico, que integre todas las instancias y múltiples partes interesadas.

Parágrafo 1. El Ministerio de Tecnologías de la Información y las Comunicaciones a través de resolución señalará las funciones que debe cumplir el Equipo de Respuesta a Incidentes de Seguridad cibernética para entidades del sector gobierno.

Parágrafo 2. El equipo de Respuesta a Incidentes de Seguridad cibernética para entidades del sector gobierno, apoyará a todas las Entidades gubernamentales, en las etapas de prevención; protección y detección; respuesta y comunicación; recuperación y aprendizaje, y para ello realizará las siguientes actividades:

ARTÍCULO 2.2.21.1.5.4. ***Equipo de Respuesta a Incidentes de Seguridad cibernética de los sectores definidos como críticos o prestadores de servicios esenciales. Csirt – Sectoriales*****.** Las organizaciones definidas como críticas o prestadoras de servicios esenciales, podrán crear Equipos de Respuesta a Incidentes de Seguridad cibernética de su sector. Para ello, deberán contar con recursos humanos, técnicos, administrativos y operativos que les permitan cumplir con las actividades derivadas de dicha actividad.

ARTÍCULO 2.2.21.1.5.5. ***Cooperación y coordinación de los CSIRT sectoriales*****.** El Ministerio de Tecnologías de la Información y las Comunicaciones en coordinación con los equipos de respuesta a incidentes establecerá a mas tardar el 1 de febrero de 2023, un protocolo de gestión de incidentes de seguridad digital nacional, que determine los roles, responsabilidades, mecanismos de coordinación, canales de comunicación y tiempos de respuesta que deberán cumplir cada uno de los equipos.

ARTÍCULO 2.2.21.1.5.6. ***Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.*** El Ministerio de Tecnologías de la Información y las Comunicaciones por medio del COLCERT pondrá a disposición de todos los actores involucrados la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

1. La plataforma permitirá el intercambio de información y el seguimiento de incidentes entre los operadores de servicios esenciales o proveedores de servicios digitales, las autoridades competentes y los CSIRT sectoriales de manera segura y confiable, sin perjuicio de los requisitos específicos que apliquen en materia de protección de datos de carácter personal.
2. La plataforma deberá garantizar la disponibilidad, autenticidad, integridad y confidencialidad de la información, y podrá emplearse para dar cumplimiento a la exigencia de notificación derivada de regulaciones sectoriales
3. La plataforma dispondrá de diversos canales de comunicación para su uso.
4. La plataforma garantizará el acceso de las autoridades competentes a toda la información relativa a la notificación y estado de situación de los incidentes de su ámbito de competencia, que les permita efectuar su adecuado seguimiento . Igualmente, las autoridades competentes tendrán

"

acceso a través de la plataforma a datos estadísticos, en particular a los necesarios para generar los informes en el marco de sus responsabilidades y funciones.

5. La plataforma implementará el procedimiento de notificación y gestión de incidentes y dispondrá como mínimo de las siguientes capacidades:

    5.1. Gestión de ciberincidentes, con incorporación de taxonomía, criticidad y notificaciones a terceros.
    5.2. Intercambio de información sobre ciberamenazas.
    5.3. Análisis de muestras.
    5.4. Registro y notificación de vulnerabilidades.
    5.5. Comunicaciones seguras entre los actores involucrados en diferentes formatos y plataformas.
    5.6. Intercambio masivo de datos.
    5.7. Generación de estadísticas e informes agregados

ARTÍCULO 2.2.21.1.5.7. *intercambio de información.* Los equipos de respuesta a incidentes de seguridad digital deberán priorizar acciones para facilitar el intercambio de información entre estos, así como con otras partes interesadas sobre amenazas, vulnerabilidades e incidentes, con el fin de desarrollar capacidades de análisis y prevención de incidentes cibernéticos.

ARTÍCULO 2. *Vigencia.* El presente Decreto rige a partir de su publicación en el Diario Oficial, y 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.

PUBLÍQUESE Y CÚMPLASE

Dado en Bogotá D.C. a los

La Ministra de Tecnologías de la Información y las Comunicaciones,

CARMEN LIGIA VALDERRAMA ROJAS

“

“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 cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital”

El Ministro de Defensa Nacional,

DIEGO ANDRÉS MOLANO APONTE

El Director del Departamento Administrativo de la Función Pública,

NERIO JOSÉ ALVIS BARRANCO