Función Pública

Decreto 338 de 2022

DECRETO 338 DE 2022

(8 DE MARZO)

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN

COMUNICACIONES

"Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones"

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 y el artículo 43 de la Ley 489 de 1998,

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 en materia de seguridad digital.

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, numeral 2, 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 del decreto en mención 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 es la de "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.

Que, mediante la Política Nacional de Seguridad digital, contenida en el Conpes 3854 del 11 de abril de 2016, 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 para la Transformación Digital y Gestión y Cumplimiento 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 encuentra 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 deberán implementar 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 estableció, a través dela Resolución 500 de 2021 los lineamientos y estándares para la estrategia de seguridad digital, y la adopción del Modelo de Seguridad y Privacidad de la Información - MSPI, como habilitador de la política de Gobierno Digital., 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 el objetivo de 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.

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 18 de febrero de 2022.

Que, 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:

"TITULO 21

LINEANIIENTOS 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 64 de la Ley 1437 de 2011, 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, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras criticas 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 a 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. Para los efectos del presente se les dará el nombre de autoridades.

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, 209 de la Constitución Política, y demás normas concordantes.

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, podrán aplicar las disposiciones contenidas en este decreto, siempre que no resulten contrarias a su naturaleza y a las disposiciones que regulan su actividad o servicio. En cualquier caso, las personas jurídicas de derecho privado sujetarán sus actuaciones a las disposiciones especiales que regulen su actividad o servicio.

PARÁGRAFO 3. Las entidades de regulación, en el marco de sus competencias, evaluarán la necesidad de expedir normas para la protección de las infraestructuras criticas cibernéticas o de los servicios esenciales de su sector. Las entidades de supervisión, en el marco de sus competencias, evaluarán la necesidad de proferir instrucciones a sus vigiladas para el mismo fin.

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, por su sigla en inglés. Es el equipo que dispone de la capacidad centralizada para la coordinación de gestión de incidentes de seguridad digital.

2. Ciberespacio: Red interdependiente de infraestructuras de tecnología de la información que incluye Internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores integrados en industrias.

3. Ciberdefensa: Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. Implica el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética.

4. CSIRT: (Computer Security lncident & Response Team) Equipo de Respuesta a Incidentes de Seguridad Cibernética, por su sigla en inglés. Es el equipo que provee las capacidades de gestión de incidentes a una organización/sector en especial. Esta capacidad permitir 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.

5. CSIRT sectorial: Son los equipos de respuesta a incidentes de cada uno de los sectores, para el adecuado desarrollo de sus actividades económicas y sociales, a partir del uso de las tecnologías de la información y las comunicaciones.

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

7. Gobernanza de la seguridad digital para Colombia: Corresponde al conjunto de interacciones y enfoques entre las 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.

8. Incidente de seguridad digital: Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable.

9. Infraestructura crítica cibernética: Sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía.

10. Modelo de Gobernanza de Seguridad digital: Es el esquema de trabajo compuesto por un conjunto de políticas de operación, principios, normas, reglas, procedimientos de toma de decisiones y programas compartidos por las múltiples partes interesadas de la seguridad digital del país, 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: Corresponde al conjunto de actores que dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales. Comprende a las autoridades, las organizaciones privadas, los operadores o propietarios de las infraestructuras críticas cibernéticas nacionales, los prestadores de servicios esenciales, la academia y la sociedad civil.

12. Riesgo de seguridad digital: Es la combinación de amenazas y/o vulnerabilidades que se pueden materializar en el curso de cualquier actividad en el entorno digital y que puede afectar el logro de los objetivos económicos o sociales al alterar la confidencialidad, integridad y disponibilidad.

13. Seguridad de la información: Preservación de la autenticidad, confidencialidad, integridad, y disponibilidad de la información, 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, a través de la apropiación de políticas, 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; que demanda la voluntad social y política de las múltiples partes interesadas.

15. Servicio esencial: En el marco de la gestión de riesgos de la seguridad digital es aquel 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.* Las autoridades 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 gestión y 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, 2º de la Ley 1341 de 2009, 3º de la Ley 1437 de 2011, 4º de la Ley 1581 de 2012, los atinentes a la Política de Gobierno Digital contenidos en el artículo 2.2.9.1.1.3 del Decreto 1078 de 2015, y los principios de gestión documental contenidos en el artículo 2.8.2.8.5.5 del Decreto 1080 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 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, Las autoridades aunarán esfuerzos para el logro de los objetivos institucionales o comunes.

5. Enfoque basado en la gestión de riesgos. Las autoridades 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. Las autoridades desarrollarán 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 y protección del ciberespacio.

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

8. Proporcionalidad. Las acciones y operaciones en el ciberespacio serán proporcionales 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. 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, primará la alternativa de solución más garantista en el marco del respeto por los derechos humanos, la libre competencia económica, y valores incorporados en la Constitución Política y los tratados internacionales ratificados por Colombia.

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

SECCIÓN 2

MODELO DE GOBERNANZA DE SEGURIDAD DIGITAL

ARTÍCULO 2.2.21.1.2.1. *Modelo de Gobernanza* de *la Seguridad Digital.* Las autoridades adoptarán el modelo de gobernanza descrito en la presente sección y, desde sus competencias, aplicarán los objetivos, principios, niveles e instancias, que permitan su materialización, con el fin de fortalecer la seguridad digital, la protección de las redes, las infraestructuras críticas, los servicios esenciales y los sistemas de información en el ciberespacio.

Parágrafo. El Ministerio de Tecnologías de la Información y las Comunicaciones señalará los lineamientos y estándares que deberán cumplir las autoridades para la adopción del modelo de gobernanza de que trata la presente sección, en los términos establecidos en el título 9 del Decreto 1078 de 2015.

ARTÍCULO 2.2.21.1.2.2. *Objetivos del Modelo de Gobernanza de la Seguridad Digital:* El Modelo de Gobernanza de la Seguridad Digital 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 integral para Ta 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 de la Seguridad Digital.* 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

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. Coordinación Nacional de Seguridad Digital.

2. Comité 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. *Coordinación Nacional* de *Seguridad Digital:* El Presidente de la República designará al responsable de la Coordinación Nacional de Seguridad Digital el cual será la persona o dependencia responsable de coordinar los asuntos de seguridad digital en el Gobierno Nacional.

ARTÍCULO 2.2.21.1.3.3. *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.

7. Promover el respeto a los derechos humanos en las actividades realizadas en el marco de la seguridad digital del país.

ARTÍCULO 2.2.21.1.3.4. *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 el entorno digital.

ARTÍCULO 2.2.21.1.3.5. 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 Relaciones Exteriores o su delegado.

3. El Ministro de Hacienda y Crédito Público o su delegado.

4. El Ministro de Justicia y del Derecho o su delegado.

5. El Ministro de Defensa Nacional o su delegado.

6. El Ministro de Minas y Energía o su delegado.

7. El Ministro de Salud y Protección Social o su delegado.

8. El Ministro de Educación Nacional o su delegado.

9. Ministerio de Ambiente y Desarrollo Sostenible o su delegado.

10. El Ministro de Vivienda, Ciudad y Territorio o su delegado.

11. El Ministro de Tecnologías de la Información y las Comunicaciones o su delegado.

12. El Ministro de Transporte o su delegado.

13. El Ministro de Cultura o su delegado.

14. El Ministro de Ciencia Tecnología e Innovación o su delegado.

15. El Director del Departamento Nacional de Planeación o su delegado.

16. El Director del Departamento Administrativo Nacional de Estadística o su delegado.

17. El Comandante General de las Fuerzas Militares o su delegado.

18. El Director General de la Policía Nacional o su delegado.

19. El Director de la Dirección Nacional de inteligencia o su delegado.

20. Un representante de las autoridades de cada uno de los sectores catalogados como titulares de infraestructura crítica cibernética o de servicios esenciales.

PARÁGRAFO 1. Los delegados al Comité Nacional de Seguridad digital deberán 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.

PARÁGRAFO 2. El Comité Nacional de Seguridad Digital, ocasionalmente, podrá invitar a sus reuniones a representantes de otras entidades, expertos en la materia, academia, sociedad civil y a representantes del sector privado.

PARÁGRAFO 3. El Comité Nacional de Seguridad Digital coordinará con las Ramas Legislativa y Judicial, los órganos de control, los autónomos e independientes, demás órganos del Estado e instancias existentes, las actividades que permitan garantizar la seguridad digital.

ARTÍCULO 2.2.21.1.3.6. *Funciones del Comité Nacional* de *Seguridad Digital:*

Son funciones del Comité Nacional de Seguridad Digital

1. Recomendar al gobierno, 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.

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 al gobierno 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.

4. Presentar al gobierno las 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 de funcionamiento, en el marco de sus competencias.

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. Promover el respeto a los derechos humanos en las actividades realizadas en el marco de la seguridad digital.

10. Las demás que sean señaladas en normas especiales.

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, mejorar la cooperación internacional, y promoverán el respeto a los derechos humanos en las actividades realizadas en el marco de la seguridad digital.

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 que 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. Los espacios técnicos propenderán para que toda la actividad realizada sea bajo el respeto de los derechos humanos.

PARÁGRAFO. El Ministerio de Tecnologías de la Información y las Comunicaciones orientará a los Comités Sectoriales y los Comités Departamentales, Distritales y Municipales de Gestión y Desempeño en la implementación y operación de las políticas de seguridad digital.

Artículo 2.2.21.1.3.9. *Puestos* de *Mando Unificado* che *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. Las autoridades que intervengan en los puestos de mando unificado lo harán para el cumplimiento coordinado de las funciones que señala la constitución, la ley, y bajo el respeto y protección de los derechos humanos.

SECCIÓN 4

IDENTIFICACIÓN DE INFRAESTRUCTURAS CRÍTICAS CIBERNÉTICAS Y SERVICIOS ESENCIALES

ARTÍCULO 2.2.21.1.4.1. *Infraestructuras críticas cibernéticas y servicios esenciales.* El Ministerio de Tecnologías de la Información y las Comunicaciones, levantará el inventario de infraestructuras críticas públicas cibernéticas nacionales y de servicios esenciales en el ciberespacio. Dicho inventario se deberá actualizar como mínimo una vez cada dos años.

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 autoridad 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.

2. La prestación de dicha actividad o servicio depende de las redes y sistemas de información, 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. Dentro de los doce (12) meses siguientes a la expedición del presente decreto, el Ministerio de Tecnologías de la Información y las Comunicaciones definirá la metodología para realizar el levantamiento del inventario de infraestructuras críticas cibernéticas y de servicios esenciales a cargo de las autoridades, y deberá incorporar las mejores prácticas que le sean aplicables. Dicha metodología incorporará el mecanismo a través del cual se seleccionará el representante de las autoridades de cada uno de los sectores catalogados como titulares de infraestructura crítica cibernética o de servicios esenciales, ante el Comité Nacional de Seguridad Digital.

ARTÍCULO 2.2.21.1.4.2. *Vinculación de los sectores críticos y prestadores de* servicios *esenciales.* Las autoridades que sean identificadas 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 Tecnologías de la Información y las Comunicaciones - Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT)

El Ministerio de Tecnologías de la Información y las Comunicaciones señalará los lineamientos y estándares que deberán cumplir las autoridades para el proceso de vinculación, en los términos establecidos en el titulo 9 del Decreto 1078 de 2015.

El proceso de intercambio de información se realizará dando cumplimiento a la política de gobierno digital, particularmente, a los habilitadores de arquitectura, servicios ciudadanos digitales, y, seguridad y privacidad de la información.

ARTÍCULO 2.2.21.1.4.3. *Obligaciones de seguridad de las autoridades titulares de infraestructura crítica, o que presten* servicios esenciales. Las autoridades, definidos como titulares de infraestructura crítica o que presten 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. Para lo anterior, deben contar con normas, políticas, procedimientos, recursos técnicos, administrativos y humanos necesarios para gestionar efectivamente el riesgo, 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

El Ministerio de Tecnologías de la información y las Comunicaciones determinará los umbrales y variables cualitativas o cuantitativas de una afectación significativa, teniendo en cuenta 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 podría tener un incidente de seguridad digital, 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 de seguridad digital.

6. La puesta en riesgo o violación a los derechos humanos que se podría ocasionar.

7. La capacidad 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 - Equipo de Respuesta a Emergencias Cibernéticas de Colombia, el CSIRT — Gobierno — Equipo de Respuesta a Incidentes de Seguridad digital de Gobierno, CSIRT — Defensa - Equipo de Respuesta a Incidentes de Seguridad digital del sector Defensa, el CSIRT del Sector Inteligencia, los CSIRT — Sectoriales - Equipos 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 – Equipo de Respuesta a Emergencias Cibernéticas de Colombia.* El Ministerio de Tecnologías de la Información y las Comunicaciones coordinará el Equipo 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, el COLCERT es el punto único de contacto y respuesta nacional que coopera y ayuda a responder de forma rápida y eficiente a los incidentes de seguridad digital y a gestionar de forma activa las amenazas de seguridad digital, incluyendo la coordinación a nivel nacional e internacional de las distintas capacidades de respuesta a incidentes o Centros de Operaciones de Seguridad Digital existentes.

PARÁGRAFO. El Ministerio de Tecnologías de la Información y las Comunicaciones señalará las actividades que debe cumplir el COLCERT — Equipo de Respuesta a Emergencias Cibernéticas de Colombia.

ARTÍCULO 2.2.21.1.5.3. *Equipo de Respuesta a Incidentes de Seguridad Digital 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 Digital para las autoridades a que hace referencia el artículo 2.2.9.1.1.2. del presente 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.

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 Modelo de Seguridad y Privacidad de la Política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones. 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 las múltiples partes interesadas.

PARÁGRAFO 1. El Ministerio de Tecnologías de la Información y las Comunicaciones señalará las actividades que debe desarrollar el Equipo de Respuesta a Incidentes de Seguridad digital para entidades del sector gobierno (CSIRT - GOBIERNO).

PARÁGRAFO 2. El Equipo de Respuesta a Incidentes de Seguridad digital para entidades del sector gobierno (CSIRT - GOBIERNO), apoyará a todas las autoridades, en las etapas de prevención; protección y detección; respuesta y comunicación; recuperación y aprendizaje.

Artículo 2.2.21.1.5.4. *Equipo de Respuesta a Incidentes de Seguridad cibernética de los sectores definidos como críticos o prestadores de servicio esenciales - (CSIRT - SECTORIALES).* El Ministerio de Tecnologías de la Información y las Comunicaciones acompañará a las organizaciones definidas como críticas o prestadoras de servicios esenciales, frente a la necesidad de crear Equipos de Respuesta a Incidentes de Seguridad cibernética de su sector, o cuando cuenten con estos.

PARÁGRAFO. Los equipos de Respuesta a Incidentes de Seguridad cibernética, CSIRT - Sectoriales, sujetarán sus actuaciones a las disposiciones especiales que regulen su actividad o servicio. El Ministerio de Tecnologías de la Información y las Comunicaciones, a través del Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT) promoverá la participación, colaboración y cooperación de los equipos de Respuesta a Incidentes de Seguridad cibernética, CSIRT — Sectoriales, con el fin de intercambiar información para la gestión de amenazas e incidentes de Seguridad digital.

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 dentro de los doce (12) meses siguientes a la expedición del presente decreto, un protocolo que incorpore los lineamientos y estándares 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. *Modelo Nacional de Atención y Gestión de incidentes.* El Ministerio de Tecnologías de la Información y las Comunicaciones definirá los lineamientos y estándares que debe incorporar el Modelo Nacional de Atención y Gestión de incidentes de seguridad digital, en los términos establecidos en el título 9 del Decreto 1078 de 2015.

ARTÍCULO 2.2.21.1.5.7. *Cultura y apropiación.* Las autoridades propenderán por fortalecer la educación, capacitación, concienciación y apropiación de la seguridad digital al interior de sus organizaciones y en sus relaciones con los distintos grupos de interés. Incentivarán la generación y desarrollo de capacidades a través de centros de excelencia en seguridad digital. Cuando Las autoridades apliquen modelos de madurez de seguridad digital considerarán la incorporación de la cultura organizacional como uno de los elementos a evaluar.

ARTÍCULO 2.2.21.1.5.8. *Seguridad y privacidad en el proceso de identificación* y gestión *de incidentes.* En el proceso de identificación y gestión de incidentes, Las autoridades deberán garantizar el cumplimiento de las normas de protección de datos personales contenidas en las leyes 1581 de 2012, 1712 de 2014, y 1266 de 2008, cuando aplique, y las normas que la desarrollan, modifican, adicionan o sustituyan. En los casos en que las autoridades realicen recolección, procesamiento o tratamiento de datos personales, deberán adoptar medidas de responsabilidad demostrada para garantizar el debido tratamiento de dicha información, estas medidas deben ser apropiadas, efectivas, útiles, eficientes y demostrables.

ARTÍCULO 2.2.21.1.5.9. *Plataforma Nacional de Notificación y Seguimiento de Incidentes de Seguridad Digital.* 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 Incidentes de seguridad digital.

1. La plataforma permitirá el intercambio de información y el seguimiento de incidentes entre los prestadores de servicios esenciales o titulares de infraestructura crítica, 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 Incidentes de seguridad digital, con incorporación de taxonomía, criticidad y notificaciones a terceros.

5.2. Intercambio de información sobre ciber amenazas.

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 2.2.21.1.5.10. *intercambio y reporte 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.

PARÁGRAFO. Las autoridades deberán reportar los incidentes de seguridad digital a las autoridades competentes. Ante incidentes de seguridad digital, que puedan llegar a ser constitutivas de conductas punibles, se deberá priorizar la realización de la denuncia ante las autoridades competentes y en el marco de los procedimientos que para el efecto dispongan los órganos de investigación.

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

Dado en Bogotá D.C. a los 8 días del mes de Marzo de 2022.

EL PRESIDENTE DE LA REPÚBLICA

(FDO) IVAN DUQUE MARQUEZ

LA MINISTRA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIÓNES

CARMEN LIGIA VALDERRAMA ROJAS

EL DIRECTOR DEL DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPÚBLICA

VICTOR MANUEL MUÑOZ RODRIGUEZ

EL DIRECTOR DEL DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA

NERIO JOSÉ ALVIS BARRANCO

Fecha y hora de creación: 2024-10-11 12:58:36