Decreto 338 de 2022

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

Lisseth Orduz
Luis Cardenas

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 seguridaddigital, la identificación de infraestructuras criticascibernéticas y serviciosesenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital

Ámbito de aplicación

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.

Paragrafo 1: Ramas Legislativa y Judicial, en los órganos de control, en los autónomos e independientes y demás organismos del Estado

Paragrafo 2: las personas jurídicas de derecho privado sujetarán sus actuaciones a las disposiciones especiales que regulen su actividad o servicio. (siempre que no resulten contrarias a su naturaleza y a las disposiciones que regulan su actividad o servicio.)

Paragrafo 3: Las entidades de supervisión, en el marco de sus competencias, evaluarán la necesidad de proferir instrucciones a sus vigiladas para el mismo fin.

Definiciones

CERT: (Computer Emergency Response Team) Es el equipo que dispone de la capacidad centralizada para la coordinación de gestión de incidentes de seguridad digital.

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

Ciberdefensa: Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética.

CSIRT: (Computer Security Incident & Response Team) Esta capacidad permitir minimizar y controlar el daño resultante de incidentes, proveyendo la respuesta, contención y recuperación efectiva, así como trabajaren pro de prevenir la ocurrencia de futuros incidentes.

Definiciones

CSIRT sectorial: Equipos de respuesta a incidentes de cada uno de los sectores, para el adecuado desarrollo de sus actividades económicas y sociales.

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

Gobernanza de la seguridad digital para Colombia: Conjunto de interacciones y enfoques entre las múltiples partes interesadas para identificar, enmarcar, proponer, y coordinar respuestas proactivas y reactivas a posibles amenazas

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

Definiciones

Infraestructura crítica cibernética: Sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un impactograve en el bienestar social

Modelo de Gobernanza de Seguridad digital: 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.

Múltiples partes interesadas: Corresponde al conjunto de actores que dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales.

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

Definiciones

Seguridad de la información: Preservación de la autenticidad, confidencialidad, integridad, y disponibilidad de la información, en cualquier medio de almacenamiento:

Seguridad digital: Es la situación de normalidad y de tranquilidad en el entorno digital, a través de la apropiación de políticas, buenas prácticas

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

Vulnerabilidad de seguridaddigital: Debilidad, atributoo falta de aplicación de un controlque 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

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.

Principios.

Confianza: La seguridaddigital debe fomentarla confianza

Coordinación. Las actuaciones que se realicen en materia de seguridad digital deberán integrar de manera coordinada a las múltiples partes interesadas

Colaboración entre las múltiples partes interesadas: En la aplicación e interpretación de los presentes lineamientos se deben involucrar activamentea las múltiples partes interesadas

Principios.

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.

Enfoque basado en la gestión de riesgos. Las autoridades deben gestionar el riesgo de forma que el uso de tecnologías de la infor**mación y las comunicaciones fomente la confianza en el entorno digital**

Gradualidad. Las autoridades desarrollarán herramientas estratégicas y operativas, de alcance definido en tiempo, espacio y recursos presupuestales

Inclusión. La seguridad digital debe incluir a todas las partes interesadas

Principios.

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

Salvaguarda de los derechos humanos y los valores fundamentales de los ciudadanos.

Uso eficiente de la infraestructura y de los recursos para protección de las infraestructuras críticas cibernéticas y los servicios esenciales.

Objetivos del Modelo de Gobernanza de la Seguridad Digital

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

2. Impulsar un enfoque integralpara Ta gestión de riesgos de Seguridaddigital.

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

4. Promover la confianza para el intercambio de información y la gestióndel conocimiento sobre seguridad digitalen el país.

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

Texto

Niveles del Modelo de Gobernanza de la Seguridad Digital

1.**Nivel estratégico:** 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: 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: Se implementan y llevan a cabo actividades y tareas rutinarias definidas por el nivel táctico.

Texto

Instancias de decisión del Modelo de Gobernanza

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.

¡Gracias!