El futuro digital es de todos

MinTIC

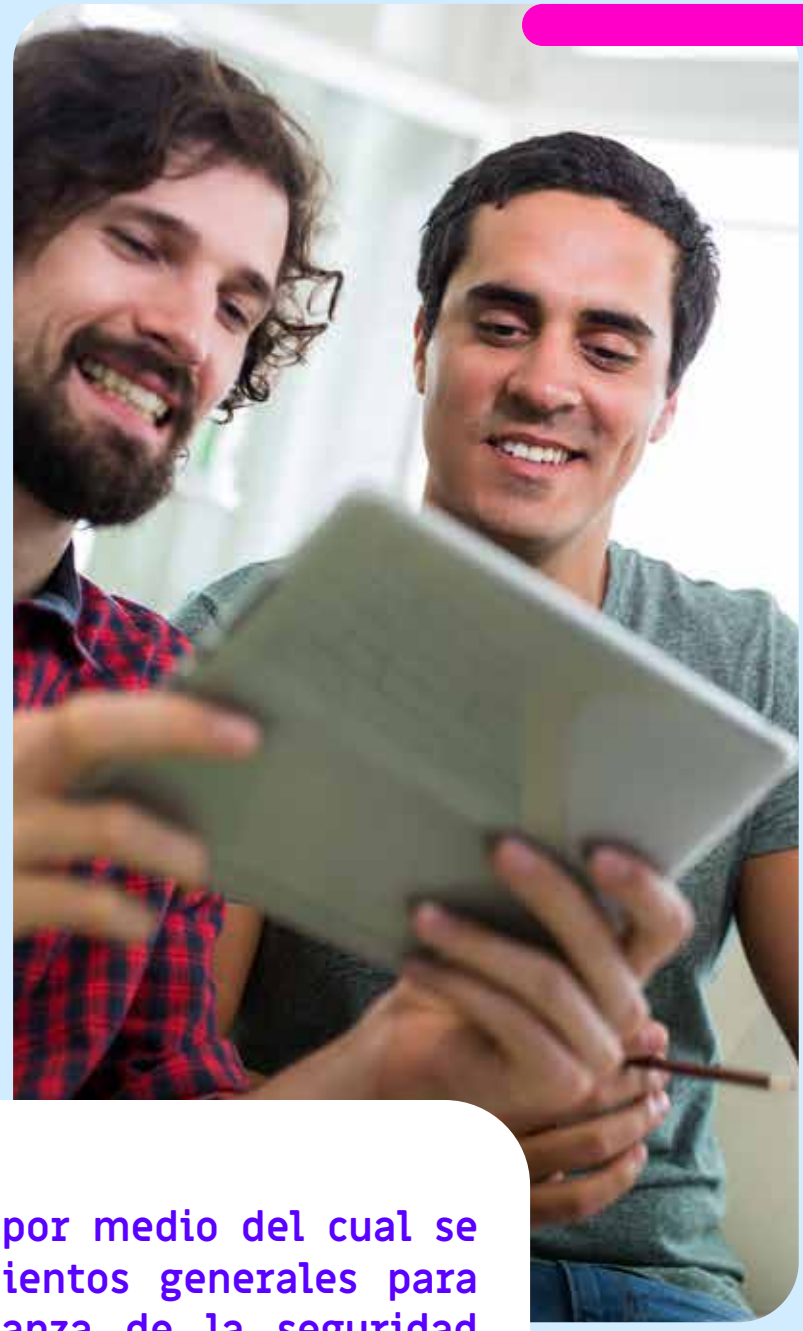
ABC

Decreto de

SEGURIDAD DIGITAL

Decreto 338 de 2022

Hechos QUE CONECTAN



Decreto 338 de 2022 por medio del cual se establece 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.

¿EN QUÉ CONSISTE?

1. Materializa los esfuerzos frente a la implementación de la política pública de Seguridad Digital.

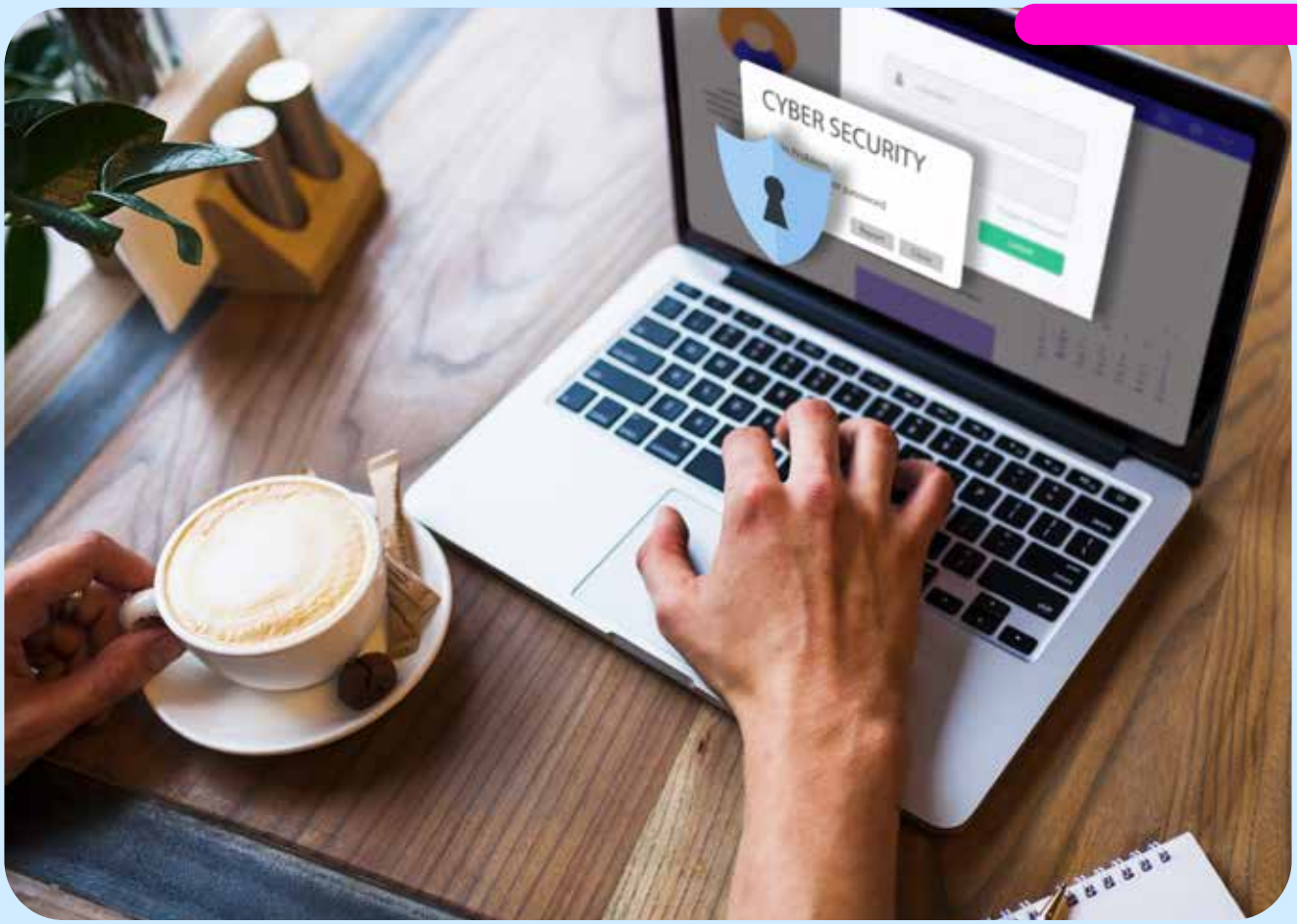
2. Permite formalizar roles y responsabilidades de quienes tienen tareas directas en este esquema de trabajo que busca no solo dictar lineamientos, sino abrir espacios de cooperación armónica entre los diferentes actores y establecer capacidades operativas que apoyen la toma de decisiones.

3. Promueve espacios para la toma de conciencia frente a la responsabilidad que tenemos todos en la correcta gestión de riesgos de seguridad.

4. Como Gobierno, ser capaces de enfrentar de manera efectiva los retos que trae el uso del entorno digital.

¿QUÉ ES LA GOBERNANZA DE LA SEGURIDAD DIGITAL?

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.



¿QUÉ ES UN MODELO DE GOBERNANZA?

Es un elemento fundamental para lograr que las múltiples partes de los actores digitales públicos tengan una coordinación efectiva en materia de seguridad digital y de esta manera, fortalecer la confianza en los ciudadanos.

Con el Decreto se pretende fortalecer la gestión de los riesgos de seguridad digital para los servicios esenciales e infraestructuras criticas cibernéticas de Colombia. Ahora bien, con el fin de mejorar la atención y respuesta a incidentes, el Decreto modifica la organización y operación del grupo interno de trabajo de respuesta a emergencias cibernéticas de Colombia (COLCERT). Todo lo anterior le apunta a un gran objetivo y es que Colombia continúe incrementando la confianza y mejorando la seguridad digital para maximizar la generación de valor socioeconómico a través de Internet y el ciberespacio.

¿CUÁLES SON LAS RESPONSABILIDADES DE LOS EQUIPOS DE RESPUESTA A INCIDENTES CIBERNÉTICOS?

Grupo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT:
Asesora, apoya y coordina 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 coopera y ayuda a responder de forma rápida y eficiente a los incidentes de seguridad digital.

Equipo de Respuesta a Incidentes de Seguridad Cibernética - CSIRT GOBIERNO:
Equipo de Respuesta a Incidentes de Seguridad Digital para las autoridades de la administración pública 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.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Edificio Murillo Toro Cra. 8 entre calles 12A y 12B
Bogotá, D.C. - Colombia - Código Postal 111711
Tel: (+57) 601 344 34 60 - Línea Gratuita: 01-800-0914014
Correo: minticresponde@mintic.gov.co
Horario de Atención:
Lunes a Viernes 8:30 am - 4:30 p.m.

www.mintic.gov.co

Hechos QUE CONECTAN