POLÍTICA DE DATOS ABIERTOS

La Curadora Urbana No. 2 de Cajicá, Arq. Andrea Parra Rojas, por medio del presente documento establece la política de datos abiertos del sitio Web de su despacho la cual se desarrolla de la siguiente manera:

OBJETIVO:

Promover la transparencia en el acceso a la información propendiendo por la publicación de información veraz, pertinente y de calidad que permita la fácil orientación a los usuarios optimizando cada uno de los procesos que deben adelantar en el despacho de la Curadora Urbana No. 2 de Cajicá y los procesos derivados de los Actuaciones que allí se lleven a cabo, siempre bajo los principios de disponibilidad, integridad y confidencialidad en la información.

ALCANCE:

El alcance de la política de seguridad digital propende por garantiza la prestación continua del servicio protegiendo la información y minimizando los riesgos que puedan llegar a presentarse.

DEFINICIONES:

- **ACTIVO DE INFORMACIÓN:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **AMENAZAS:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **ANÁLISIS DE RIESGO:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **RIESGO:** es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas.
- **RIESGO DE SEGURIDAD DIGITAL:** es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan.
- **GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL:** es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y

sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.

- **SEGURIDAD DE LA INFORMACIÓN:** Este habilitador busca que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad, y privacidad de la información, así como la protección de los datos personales que tratan las entidades públicas en cumplimiento de la normatividad de protección de datos personales; este habilitador tiene su soporte en el MSPI.

POLITICA:

El objetivo principal de la política de seguridad digital consiste en fortalecer 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, así como en la creación e implementación de instrumentos de resiliencia, recuperación y respuesta nacional en un marco de cooperación, colaboración y asistencia.

Esta política se desarrollará a través de las siguientes acciones:

- Fortalecer las capacidades en seguridad digital
- Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad
- Definir indicadores para medir la eficiencia y eficacia del sistema de gestión de seguridad y privacidad de la información
- Establecer un marco institucional articulado que involucre a las múltiples partes interesadas para la implementación de la política de seguridad digital
- Establecer mecanismos de participación activa y permanente de las múltiples partes interesadas en la gestión del riesgo de seguridad digital
- Generar confianza en las múltiples partes interesadas en el uso del entorno digital