1. Introducción y Marco Normativo

- **Objeto:** Establecer las políticas, procedimientos y directrices para el **tratamiento** de los Datos Personales (DP) y la información financiera, crediticia, comercial y de servicios (Hábeas Data Financiero) recolectados por la organización, garantizando el derecho fundamental al Hábeas Data.
- **Alcance:** Aplica a todo tratamiento de DP realizado por la organización, sus empleados, contratistas y terceros que actúen por cuenta de esta.
- **Marco Legal:**
  - **Ley 1581 de 2012:** Disposiciones generales para la protección de DP.
  - **Decreto 1377 de 2013** (y normas modificatorias): Reglamentación parcial de la Ley 1581.
  - **Ley 1266 de 2008:** Disposiciones generales del Hábeas Data y regulación de la información financiera, crediticia, comercial y de servicios.
  - **Ley 2157 de 2021** (Ley de Borrón y Cuenta Nueva): Modificación y adición a la Ley 1266.

2. Definiciones Clave

Se deben incluir definiciones claras y sencillas (basadas en la ley) para conceptos como:

- **Dato Personal (DP):** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (ej. nombre, cédula, correo, teléfono).
- **Dato Sensible:** Aquel que afecta la intimidad del Titular o cuyo uso indebido puede generar discriminación (ej. origen racial o étnico, opiniones políticas, estado de salud, datos biométricos).
- **Titular:** Persona natural o jurídica a quien se refiere la información.
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre los DP (recolección, almacenamiento, uso, circulación o supresión).
- **Responsable del Tratamiento:** La organización que decide sobre la base de datos y/o el tratamiento de los datos.
- **Encargado del Tratamiento:** Persona natural o jurídica que realiza el tratamiento de datos por cuenta del Responsable (ej. un proveedor de *hosting*).

3. Principios Aplicables al Tratamiento

El tratamiento debe regirse por los siguientes principios:

- **Legalidad:** El tratamiento debe sujetarse a lo establecido en la ley.

- **Finalidad:** Los datos se recolectan y usan para un propósito **específico y legítimo**, informado al Titular.
- **Libertad:** El tratamiento solo puede ejercerse con el **consentimiento previo, expreso e informado** del Titular (salvo excepciones legales).
- **Veracidad o Calidad:** La información debe ser **veraz, completa, exacta, actualizada, comprobable y comprensible.**
- **Transparencia:** Debe garantizarse el derecho del Titular a obtener información sobre sus datos.
- **Acceso y Circulación Restringida:** El tratamiento se limita a personas autorizadas y no puede estar disponible en internet de forma irrestricta.
- **Seguridad:** Deben adoptarse las medidas técnicas, humanas y administrativas para **otorgar seguridad a los registros**.
- **Confidencialidad:** La obligación de reserva se mantiene, incluso después de finalizar la relación con el tratamiento.

4. Derechos de los Titulares (ARCO)

Se debe describir el derecho fundamental a conocer, actualizar y rectificar la información, incluyendo:

- **Conocer:** Solicitar información sobre qué datos están siendo tratados y la finalidad.
- **Actualizar:** Poner al día la información.
- **Rectificar:** Corregir la información inexacta.
- **Revocar la Autorización:** Excepto en los casos previstos por la ley.
- **Suprimir:** Solicitar la eliminación de sus datos, salvo si existe un deber legal o contractual de mantenerlos.
- **Reclamar:** Presentar quejas ante la Superintendencia de Industria y Comercio (SIC).

5. Autorización del Titular

- **Requisito:** La autorización debe ser **previa, expresa e informada** para el tratamiento de DP.
- **Medio:** Puede ser por cualquier medio (escrito, verbal, electrónico) que permita su **consulta posterior**.
- **Contenido Mínimo:** Se debe informar al Titular:
    - El DP que será recolectado.
    - La **finalidad** específica del tratamiento.

- Los derechos que le asisten.
- La identificación del Responsable del Tratamiento.

6. Procedimiento para Consultas y Reclamos

- **Contacto (Área y Dirección):** Designar un área o persona responsable (ej. Oficial de Protección de Datos o área Jurídica).
- **Términos de Respuesta:**
  - **Consulta:** Máximo **diez (10) días hábiles** (prorrogable por cinco (5) días más).
  - **Reclamo (Queja):** Máximo **quince (15) días hábiles** (prorrogable por ocho (8) días más).
- **Requisitos del Reclamo:** Identificación del Titular, descripción de los hechos, dirección y documentos soporte.

7. Medidas de Seguridad y Registro Nacional de Bases de Datos (RNBD)

- **Medidas de Seguridad:** Describir las medidas **técnicas, humanas y administrativas** implementadas para la seguridad de los datos (ej. acceso restringido a bases de datos, cifrado, capacitaciones, copias de seguridad).
- **RNBD:** La **organización** debe inscribir sus bases de datos ante la SIC, especificando la finalidad y el tratamiento que se da a la información, y actualizar la información anualmente.

8. Régimen Especial para Hábeas Data Financiero (Ley 1266 de 2008)

- **Datos Positivos:** Permanecerán de manera indefinida en los bancos de datos.
- **Datos Negativos (Mora):** El tiempo de permanencia es el **doble de la mora**, máximo **cuatro (4) años** contados a partir del pago de la obligación.
- **Comunicación Previa:** La fuente de la información debe enviar una comunicación al Titular antes de reportar la información negativa.

LUIS HERNAN BONILLA CUERVO

Representante Legal