

# Decasystems SRL

## Política de Protección de Datos

### **1. Compromiso con la Protección de Datos**

En **Decasystems SRL**, reconocemos la importancia de proteger los datos personales de nuestros clientes, colaboradores y terceros. Por ello, nos comprometemos a garantizar la confidencialidad, integridad, seguridad y el uso legítimo de dichos datos, en cumplimiento con la **Ley No. 172-13 sobre Protección Integral de Datos Personales de la República Dominicana**.

### **2. Fundamento Legal**

Esta política se basa en los principios establecidos en la Ley 172-13, en especial:

- **Licitud:** Solo tratamos datos personales de forma legal y con fines legítimos.
- **Consentimiento:** No recolectamos ni procesamos datos personales sin el consentimiento expreso del titular, salvo en los casos autorizados por la ley.
- **Calidad de los Datos:** Nos aseguramos de que los datos de nuestros clientes sean veraces, pertinentes, actualizados y adecuados a la finalidad de su tratamiento.
- **Seguridad de los Datos:** Adoptamos medidas técnicas y organizativas para evitar el acceso no autorizado, alteración, pérdida o destrucción de los datos de nuestros clientes.
- **Deber de Confidencialidad:** Todos nuestros colaboradores y terceros con acceso a datos de nuestros clientes están obligados a mantener la confidencialidad, incluso después de finalizada su relación laboral o contractual.
- **Derechos del Titular:** Garantizamos el derecho de los titulares a acceder, rectificar, actualizar, suprimir u oponerse al tratamiento de sus datos .

### **3. Finalidades del Tratamiento**

Los datos de nuestros clientes que recopilamos son utilizados exclusivamente para la prestación de nuestros servicios tecnológicos, administración de relaciones contractuales, facturación, soporte técnico, cumplimiento de obligaciones legales, y otros fines previamente informados y autorizados.

### **4. Medidas de Seguridad**

Decasystems SRL dispone de controles tecnológicos y organizacionales para proteger los datos de nuestros clientes, incluyendo:

- Autenticación y control de accesos.
- Cifrado de información sensible.
- Copias de seguridad periódicas.
- Políticas internas de acceso mínimo y auditoría.