POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

Conforme a la Ley No. 172-13 de la República Dominicana

Campo	Detalle
Documento	POL-PDP-001
Versión	1.0
Fecha de emisión	Abril 2026
Clasificación	Pública — disponible para clientes y usuarios
Responsable	Dirección de Tecnología y Cumplimiento
Revisión siguiente	Octubre 2026
Marco legal	Ley No. 172-13, República Dominicana

1. Identificación del Responsable del Tratamiento

En cumplimiento de lo establecido en la Ley No. 172-13 sobre Protección de Datos de Carácter Personal de la República Dominicana, la empresa responsable del tratamiento de los datos es la entidad que suscribe los contratos de servicio con sus clientes y opera la plataforma tecnológica objeto de esta política.

> Nota importante: Los campos de nombre, dirección y datos de contacto del responsable deben ser completados con los datos registrados de su empresa ante la Cámara de Comercio y Producción correspondiente, así como ante la Dirección General de Impuestos Internos (DGII).
>
> Razón Social: Braintech Solutions SRL
> RNC: 131805345
> Domicilio: C/AMALFI, EDIF DON ALEJANDRO I APTO 2B, URBANIZACIÓN ITALIA, SANTO DOMINGO ESTE
> Correo de contacto para protección de datos: sig.donny@gmail.com

2. Marco Legal Aplicable

La presente política se fundamenta en los siguientes instrumentos legales y normativos:

Instrumento	Descripción
Ley No. 172-13	Ley sobre Protección de Datos de Carácter Personal de la República Dominicana, promulgada el 13 de diciembre de 2013.
Constitución Dominicana	Artículo 44 — Derecho a la intimidad y protección de datos personales.
Ley No. 53-07	Ley sobre Crímenes y Delitos de Alta Tecnología, que complementa la protección en entornos digitales.
Ley No. 20-00	Ley de Propiedad Industrial, aplicable a activos de información.
Normas DGII	Normativa de la Dirección General de Impuestos Internos sobre manejo de identificadores tributarios (RNC/Cédula).

3. Objeto y Ámbito de Aplicación

Esta política tiene por objeto definir los principios, compromisos y medidas técnicas adoptadas por la empresa para garantizar la privacidad, confidencialidad e integridad de los datos vinculados a sus clientes, en estricto apego a la Ley 172-13.

Esta política aplica a:

- Todos los datos procesados por la plataforma tecnológica en el contexto de la prestación del servicio.
- Los clientes (personas jurídicas) que se integran a la plataforma mediante API.
- El personal interno con acceso a sistemas de información.
- Proveedores y subencargados de tratamiento que accedan a datos en nombre de la empresa.

4. Datos que Manejamos — Principio de Minimización

4.1 Declaración de Minimización de Datos

La empresa ha adoptado como principio fundamental el tratamiento mínimo de datos personales, en concordancia con el Artículo 17 de la Ley 172-13 que establece que los datos deben ser adecuados, pertinentes y no excesivos en relación con el fin para el que se recaban.

> Declaración expresa: La plataforma NO recaba, NO almacena ni procesa datos personales de los clientes finales ni de personas naturales. El servicio está orientado exclusivamente a

personas jurídicas (empresas) y opera únicamente con los identificadores técnicos estrictamente necesarios para la prestación del servicio.

4.2 Inventario de Datos Tratados

Los únicos datos vinculados al cliente que la plataforma procesa son los siguientes:

Dato	Finalidad	Tratamiento de seguridad	Base legal (Ley 172-13)
RNC (Registro Nacional del Contribuyente)	Identificación única del cliente en el sistema para enrutamiento de transacciones.	Encriptación AES-256. El valor almacenado es un hash irreversible — no es posible identificar a qué empresa corresponde sin la clave de cifrado.	Art. 6 — Consentimiento contractual / ejecución de contrato
API Key del cliente	Autenticación y autorización de las solicitudes entrantes a la API de la plataforma.	Almacenado únicamente en forma encriptada (hash bcrypt/SHA-256). La empresa no puede recuperar el valor original.	Art. 6 — Ejecución de contrato de servicio
Contraseña de certificados digitales	Acceso a los certificados requeridos para la integración con sistemas fiscales o de terceros.	Encriptada en reposo con AES-256 y en tránsito con TLS 1.3. Acceso restringido mediante control de roles.	Art. 6 — Ejecución de contrato de servicio

La empresa NO maneja ninguno de los siguientes datos personales de personas naturales:

- Nombre, apellido o alias de personas físicas.
- Número de cédula de identidad y electoral.
- Correo electrónico personal o número de teléfono.
- Datos de salud, biométricos, financieros u otros datos sensibles.
- Dirección física o domicilio de personas naturales.
- Datos de menores de edad.

5. Anonimización y Seudonimización del RNC

5.1 Mecanismo de Encriptación del RNC

El Registro Nacional del Contribuyente (RNC) es el único identificador de persona jurídica que la plataforma procesa. En cumplimiento del principio de seguridad establecido en el Artículo 26 de la Ley 172-13, este dato es seudonimizado desde el momento de su ingreso al sistema.

Funcionamiento del RNC encriptado:

1. Al registrar un cliente, el RNC se somete a un proceso de cifrado con clave gestionada en Azure Key Vault.
2. El valor almacenado en la base de datos es el resultado cifrado — no el RNC original.
3. Internamente, cada cliente es identificado por un UUID (identificador aleatorio) generado por el sistema, completamente desvinculado del RNC.
4. Ninguna persona del equipo interno puede conocer el RNC de un cliente observando directamente la base de datos.
5. El RNC original solo puede obtenerse mediante un proceso de descifrado controlado, con registro de auditoría, disponible exclusivamente para procesos legales o fiscales que lo requieran.

Esta arquitectura garantiza que no sea posible identificar a qué empresa pertenece una transacción sin disponer de la clave de cifrado correspondiente.

5.2 Consecuencia para los Titulares

Dado que los datos de RNC son seudonimizados, la plataforma cumple con el principio de no identificabilidad directa establecido en la Ley 172-13. Los datos tratados no permiten, por sí solos, identificar a una persona jurídica o a ninguna persona natural asociada a ella.

6. Protección de Credenciales Técnicas

6.1 API Keys

Las API Keys son credenciales de autenticación asignadas a cada cliente integrado. Su tratamiento sigue el siguiente esquema de seguridad:

- Al momento de la generación, la API Key se muestra al cliente una única vez en texto claro.
- La plataforma almacena exclusivamente el hash de la API Key (algoritmo bcrypt con salt). Es imposible recuperar el valor original.
- En caso de pérdida, el cliente debe solicitar la regeneración. No existe proceso de recuperación del valor original.
- Las API Keys se transmiten únicamente sobre conexiones cifradas TLS 1.3.
- Cada uso de una API Key queda registrado en el log de auditoría con timestamp e IP de origen.

6.2 Contraseñas de Certificados Digitales

Las contraseñas asociadas a certificados digitales (p. ej., para firma electrónica o integración con la DGII) se gestionan bajo los siguientes controles:

- Almacenamiento en Azure Key Vault con cifrado AES-256 gestionado por hardware (HSM).

- Cifrado en tránsito con TLS 1.3 en todas las transmisiones.
- Acceso restringido mediante control de identidad y privilegios mínimos (principio least privilege).
- Rotación periódica de claves de cifrado conforme a política interna de gestión de claves.
- Registro de auditoría de todo acceso a credenciales almacenadas en Key Vault.

Credencial	Algoritmo de cifrado en reposo	Cifrado en tránsito	Recuperable por operador
RNC del cliente	AES-256 (Azure Key Vault)	TLS 1.3	No — solo mediante proceso legal documentado
API Key	Hash bcrypt (unidireccional)	TLS 1.3	No — debe regenerarse
Contraseña de certificado	AES-256 (Azure Key Vault)	TLS 1.3	No — acceso controlado y auditado

7. Principios del Tratamiento (Art. 17, Ley 172-13)

El tratamiento de datos que realiza la plataforma se rige por los principios establecidos en la Ley 172-13:

Principio	Artículo	Cómo lo cumplimos
Licitud	Art. 17(a)	Todo tratamiento está amparado en la relación contractual con el cliente o en obligación legal.
Finalidad	Art. 17(b)	Los datos se recopilan con fines determinados, explícitos y legítimos. No se reutilizan para fines incompatibles.
Proporcionalidad	Art. 17(c)	Solo se tratan los datos estrictamente necesarios. No se recaban datos personales de personas naturales.
Calidad	Art. 17(d)	Los datos se mantienen exactos y actualizados conforme a la información provista por el cliente.
Seguridad	Art. 26	Cifrado AES-256, TLS 1.3, Azure Key Vault, control de accesos y auditoría continua.
Confidencialidad	Art. 27	El personal con acceso a datos esta sujeto a deber de secreto profesional.
Transparencia	Art. 18	Esta política es pública y está disponible en el sitio web y en la plataforma.

8. Derechos de los Titulares (ARCO — Arts. 20-24, Ley 172-13)

La Ley 172-13 reconoce a los titulares de datos los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO). Dado que la plataforma no maneja datos de personas naturales, estos derechos aplican principalmente a los representantes legales de las personas jurídicas clientes en lo que respecta a los datos de identificación de su empresa.

Derecho	Artículo	Cómo ejercerlo	Plazo de respuesta
Acceso	Art. 20	Solicitud escrita a braintech.rd@gmail.com indicando el dato sobre el que se solicita información.	10 días hábiles
Rectificación	Art. 21	Solicitud escrita adjuntando documentación que acredite la corrección requerida.	10 días hábiles
Cancelación	Art. 22	Solicitud escrita. Aplica previa terminación del contrato y cumplimiento de obligaciones legales de retención.	30 días hábiles
Oposición	Art. 23	Solicitud escrita indicando el tratamiento específico al que se opone y el motivo.	10 días hábiles

9. Transferencia Internacional de Datos

La infraestructura de la plataforma opera en Microsoft Azure. En virtud de ello, es posible que datos sean procesados en centros de datos ubicados fuera del territorio de la República Dominicana.

La empresa garantiza que dichas transferencias cumplen con lo establecido en los Artículos 31 y 32 de la Ley 172-13, mediante los siguientes mecanismos:

- Contrato de procesamiento de datos (DPA) suscrito con Microsoft Azure, que garantiza niveles de protección equivalentes o superiores a los requeridos por la Ley 172-13.
- Los datos permanecen cifrados en todo momento, tanto en tránsito como en reposo, independientemente de su ubicación geográfica.
- La región primaria de Azure utilizada: East US seleccionada por su proximidad geográfica y nivel de certificaciones de seguridad.
- Microsoft Azure cuenta con las certificaciones ISO 27001, SOC 2 Tipo II y cumplimiento con GDPR, que son reconocidas como garantías de nivel adecuado de protección.

10. Retención y Eliminación de Datos

Dato	Período de retención	Criterio de eliminación
RNC cifrado del cliente	Durante la vigencia del contrato + 5 años	Vencido el plazo legal, eliminación segura con certificación.
API Keys (hash)	Durante la vigencia del contrato	Al terminar el contrato o al regenerar la clave.
Contraseñas de certificados	Durante la vigencia del contrato	Al terminar el contrato. Eliminación inmediata a solicitud del cliente.
Logs de auditoría	12 meses	Eliminación automática por política de retención de logs.
Datos de transacciones	5 años desde la transacción	Conforme a obligaciones tributarias y fiscales dominicanas.

11. Medidas de Seguridad Técnicas y Organizativas

11.1 Medidas Técnicas

- Cifrado en reposo: AES-256 para todos los datos sensibles mediante Azure Key Vault (HSM).
- Cifrado en tránsito: TLS 1.3 obligatorio en todas las comunicaciones de la API.
- Gestión de identidad: Autenticación multifactor (MFA) para todo acceso administrativo.
- Control de accesos: Principio de privilegio mínimo; acceso segmentado por roles.
- Monitoreo continuo: Azure Monitor y Application Insights con alertas en tiempo real.
- Alta disponibilidad: Azure App Service con zonas de disponibilidad redundantes.
- Copias de seguridad: Backups automáticos cifrados con retención definida por política.
- Pruebas de seguridad: Evaluaciones de vulnerabilidades periódicas y pruebas de penetración.

11.2 Medidas Organizativas

- Capacitación en protección de datos para todo el personal con acceso a sistemas.
- Procedimiento documentado de respuesta ante brechas de seguridad.
- Registro de actividades de tratamiento actualizado conforme al Art. 29 de la Ley 172-13.
- Revisión anual de esta política y de los controles de seguridad implementados.

12. Gestión de Brechas de Seguridad

En caso de producirse una brecha de seguridad que comprometa datos tratados por la plataforma, la empresa seguirá el siguiente protocolo, en cumplimiento con el Artículo 28 de la Ley 172-13:

Fase	Plazo	Acción
Detección y contención	0 – 2 horas	Identificación del alcance, aislamiento del sistema afectado y preservación de evidencia.
Evaluación de riesgo	2 – 24 horas	Análisis del tipo de dato comprometido, número de afectados y potencial daño.
Notificación interna	Dentro de 24 h	Informar a la Dirección
Notificación a clientes	Dentro de 72 h	Comunicar a los clientes afectados la naturaleza de la brecha, datos involucrados y medidas adoptadas.
Notificación a autoridad	Conforme a ley	Comunicar a las autoridades competentes según lo establezca la regulación vigente.
Remediación y post-mortem	Dentro de 30 d	Implementar correctivos y documentar lecciones aprendidas.

13. Subencargados del Tratamiento

La empresa utiliza los siguientes proveedores de infraestructura como subencargados del tratamiento, todos sujetos a contratos de procesamiento de datos que garantizan niveles de protección conformes a la Ley 172-13:

Proveedor	Rol	Datos que accede	Garantías
Microsoft Azure	Proveedor de infraestructura cloud	Datos cifrados en reposo y tránsito. Sin acceso al contenido.	ISO 27001, SOC 2, DPA firmado
Azure Key Vault	Gestión de claves de cifrado	Claves de cifrado (no datos de clientes directamente).	HSM certificado FIPS 140-2 Level 2

La empresa no comparte, vende ni cede datos de sus clientes a terceros con fines comerciales o de marketing.

14. Actualizaciones de esta Política

La empresa se reserva el derecho de actualizar esta política para reflejar cambios en la legislación, en los servicios ofrecidos o en las medidas de seguridad implementadas. Toda modificación será notificada a los clientes con un mínimo de 30 días de anticipación mediante correo electrónico y/o publicación en el sitio web oficial.

La versión vigente de esta política estará siempre disponible en: https://web.sigmeapps.net

Versión	Fecha	Descripción del cambio	Aprobado por
1.0	Abril 2026	Versión inicial. Publicación pública conforme a Ley 172-13.	Dirección de Tecnología y Cumplimiento