Pack de Confianza Sibell

Documento de cumplimiento, seguridad y privacidad para equipos de CISO, Compliance y Procurement

Sibell SAS

NIT: 901.916.609-5

Versión: 1.0

Fecha: 15 de mayo de 2026

Resumen Ejecutivo

Sibell SAS es una empresa colombiana que provee **infraestructura de autenticación SMS 2FA y servicios de inteligencia artificial aplicada** para fintechs, neobancos, plataformas digitales y empresas reguladas en Latinoamérica.

Este documento responde a las preguntas más frecuentes de equipos de CISO, Compliance, Legal y Procurement que evalúan a Sibell como proveedor.

Resumen en 5 puntos:

1. **Sibell opera como Encargado del Tratamiento** según la Ley 1581 de 2012. El cliente sigue siendo el Responsable de los datos de sus usuarios finales.
2. **Datos en tránsito y en reposo cifrados** (TLS 1.2+; cifrado en reposo en GCP).
3. **Códigos OTP almacenados con hash SHA-256 + salt** — nunca en texto plano.
4. **Subprocesadores listados públicamente** y bajo acuerdos de protección de datos equivalentes.
5. **Contrato de Encargo de Tratamiento (DPA) disponible** para firma desde el día uno, sin negociación pesada.

---

1. Sobre Sibell

Campo	Información
Razón social	Sibell SAS
NIT	901.916.609-5
Domicilio	Calle 174 No. 57-30, Bogotá D.C., Colombia
Año de constitución	2025
Régimen tributario	SIMPLE
Representante legal	Elimar Sibelis Pontón Deluquez
Sitio web	https://sibell.in
Contacto comercial	contacto@sibell.in
Contacto privacidad / seguridad	privacidad@sibell.in
Contacto soporte	soporte@sibell.in

Líneas de servicio

- **Verificación de identidad SMS 2FA** mediante API REST documentada con OpenAPI 3.0.
- **Inteligencia artificial aplicada:** diagnósticos, chatbots, RPA, dashboards ejecutivos.
- **Consultoría tecnológica:** roadmaps IA, arquitectura de datos, automatización.

---

2. Marco Legal y Posicionamiento como Encargado

2.1 Modelo de responsabilidad

Bajo la Ley 1581 de 2012 sobre Protección de Datos Personales en Colombia, Sibell SAS opera como **Encargado del Tratamiento**. Esto significa que:

- El **Cliente** (fintech, neobanco, plataforma) es el **Responsable del Tratamiento** de los datos personales de sus usuarios finales.
- **Sibell** recibe esos datos únicamente para enrutar los SMS de verificación, según las instrucciones del Cliente.
- Sibell **no explota** los datos personales para fines propios, no los cede a terceros distintos de los subprocesadores autorizados, y no los retiene más allá del tiempo necesario.

2.2 Documentos legales disponibles

Documento	Disponible	Ubicación
Política de Tratamiento de Datos	✅ Pública	https://sibell.in/privacidad
Términos y Condiciones del Servicio	✅ Pública	https://sibell.in/terminos
Contrato de Encargo de Tratamiento (DPA)	✅ Plantilla lista para firma	Enviado por solicitud al correo de contacto
Lista de subprocesadores	✅ Sección 4 de este documento	Actualizada con preaviso de 15 días
Procedimiento Habeas Data	✅ Documentado en Política	https://sibell.in/privacidad sección 10

2.3 Registro Nacional de Bases de Datos (RNBD)

En su rol principal de Encargado, mientras Sibell no retenga bases de datos de usuarios finales bajo responsabilidad propia, el registro RNBD ante la SIC **no resulta obligatorio**. Esta posición se revisa trimestralmente; si en el futuro Sibell construye funcionalidades que impliquen retención propia de datos personales (analítica de usuarios, dashboards con PII, etc.), se procederá al registro correspondiente.

---

3. Arquitectura de Seguridad

3.1 Infraestructura

- **Nube principal:** Google Cloud Platform (GCP)
- **Cómputo:** Cloud Run (microservicios desacoplados auth-service y verification-service)
- **Bases de datos:** Cloud SQL (PostgreSQL) con cifrado en reposo (Google-managed keys)
- **Cache distribuido:** Memorystore (Redis) para idempotencia, rate limiting y estado del circuit breaker
- **Red:** VPC privada con segmentación de servicios
- **Backups:** automáticos diarios, cifrados, con retención rotatoria documentada

3.2 Cifrado

Capa	Implementación
Cifrado en tránsito	TLS 1.2 o superior; HSTS habilitado
Cifrado en reposo	AES-256 administrado por GCP en bases de datos y backups
Códigos OTP	SHA-256 + salt antes de almacenar en Redis; comparación en tiempo constante
Credenciales / secretos	Google Secret Manager; nunca en código fuente
Tokens de pago	Tokenización Bold; Sibell no almacena PAN ni CVV

3.3 Autenticación y control de acceso

- **API Keys** asignadas por cliente, rotables desde el Dashboard.
- **JWT** para sesiones del Dashboard.
- **Hash de contraseñas** con algoritmo de un solo sentido y costo configurable.
- **Confirmación de email** en onboarding antes de habilitar producción.
- **RBAC interno** con principio de mínimos privilegios para el equipo de Sibell.
- **MFA** obligatorio para accesos administrativos a infraestructura.

3.4 Protección contra abuso

- **Phone cooldown atómico** por (API Key + número) usando Redis `SET NX`.
- **Kill-switch diario por plan** (límite de conteo de SMS).
- **Kill-switch monetario** por hora y por día (límite de costo agregado).
- **Idempotency-Key** en `/verify/send` con cache 24h — previene SMS duplicados.
- **Circuit breaker distribuido** entre proveedores SMS (CLOSED / OPEN / HALF_OPEN).
- **Failover dinámico** descarta automáticamente proveedores con baja tasa de éxito o alta latencia.

3.5 Observabilidad y auditoría

- **Logs de auditoría persistentes** en PostgreSQL (`verification_logs`) con 12 columnas: timestamp, acción, proveedor, éxito, latencia, código de error, API Key ID, teléfono enmascarado (últimos 4 dígitos).
- **Endpoint** `/metrics/providers` con success rate, latencia p95 y costo por proveedor.
- **Monitoreo automatizado** cada 5 minutos: salud de proveedores, saldos negativos, pagos pendientes; alertas por email a operaciones.
- **Reportes de uso** en CSV exportables por el cliente desde el Dashboard.

3.6 Privacidad por diseño en logs

- Los números de teléfono se almacenan **enmascarados** (visibles solo últimos 4 dígitos).
- Los códigos OTP **nunca** se almacenan en texto plano.
- Los logs de aplicación no registran PII en texto libre.

---

4. Subprocesadores

Subprocesador	Servicio prestado	País	Acuerdo de protección de datos
Inalambria Internacional S.A.S.	Enrutamiento de SMS	Colombia	Acuerdo escrito
Google LLC (Google Cloud Platform)	Infraestructura de nube	Estados Unidos	DPA estándar de Google + cláusulas contractuales
Bold Compañía de Financiamiento S.A.	Pasarela de pagos	Colombia	Términos comerciales y normativa Superfinanciera
Hostinger International Ltd.	Correo transaccional (SMTP)	Unión Europea (Lituania)	Términos del proveedor

Política de actualización: la incorporación de nuevos subprocesadores se notifica con al menos quince (15) días calendario de anticipación a los clientes, quienes pueden oponerse motivadamente.

---

5. Gestión de Incidentes

5.1 Política

Sibell mantiene una política interna de gestión de incidentes con los siguientes principios:

1. **Detección temprana** mediante monitoreo automatizado (fail rates, latencia, saldos, webhooks).
2. **Clasificación** por severidad (P1 crítico / P2 alto / P3 medio / P4 bajo).
3. **Notificación al cliente afectado en máximo 72 horas** desde el conocimiento del incidente, conforme a la cláusula correspondiente del DPA.
4. **Mitigación inmediata** según runbooks documentados.
5. **Análisis post-mortem** sin culpa, con identificación de causa raíz y acciones correctivas.
6. **Notificación a la SIC** cuando proceda, en coordinación con el cliente Responsable.

5.2 Información incluida en la notificación

- Naturaleza del incidente.

- Categorías y volumen aproximado de Titulares afectados.
- Categorías y volumen aproximado de datos afectados.
- Consecuencias probables.
- Medidas adoptadas o propuestas para mitigar.
- Punto de contacto de Sibell para información adicional.

5.3 Continuidad del servicio

- Failover automático entre proveedores SMS — si un operador degrada o falla, el siguiente del orden se activa sin intervención manual.
- Retry con backoff exponencial para errores transitorios.
- Backups diarios cifrados; pruebas periódicas de restauración.

---

6. Retención y Eliminación de Datos

Tipo de dato	Período de retención
Logs operacionales (`verification_logs`)	12 meses (configurable por contrato)
Logs de auditoría administrativa	24 meses
Backups cifrados	90 días rotatorios
Datos de facturación	Plazo legal contable (5–10 años según norma)
Datos de cuenta del cliente activo	Mientras dure la relación contractual

Al terminar el contrato, los datos se devuelven al cliente en formato exportable **o** se suprimen de forma segura, a elección del cliente, dentro de los 30 días siguientes (cláusula 12 del DPA).

---

7. SLA y Disponibilidad

Métrica	Objetivo
Uptime objetivo	99,5% mensual
Latencia p95 envío SMS	< 3 segundos
Tasa de entrega SMS	≥ 95% (dependiente de operadores)
MTTR incidente	< 2 horas en horario laboral
Tiempo de respuesta soporte	< 4 horas en horario laboral

Detalles completos del SLA, exclusiones y compensaciones en https://sibell.in/terminos (cláusula 10).

---

8. Certificaciones, Auditorías y Roadmap de Cumplimiento

8.1 Estado actual

Sibell SAS es una empresa en fase de lanzamiento comercial. Actualmente **no cuenta con certificaciones ISO 27001 ni SOC 2** formales. Las prácticas de seguridad descritas en este documento se aplican y se auditan internamente.

8.2 Roadmap

- **Mes 1–6:** consolidación de operación con clientes piloto y formalización de runbooks.
- **Mes 6–12:** evaluación de auditoría ISO 27001 o SOC 2 Type I, dependiendo del perfil de los primeros clientes corporativos.
- **Mes 12+:** auditoría formal y obtención de certificación según el segmento objetivo.

8.3 Auditorías por parte del cliente

Conforme a la cláusula 13 del DPA, el cliente puede:

- Solicitar cuestionarios de seguridad (respondidos en máximo 30 días).
- Revisar documentos de cumplimiento que Sibell ponga a disposición.
- Realizar auditoría in situ o remota una vez al año con preaviso de 30 días.

---

9. Continuidad del Negocio

- Backups cifrados diarios con retención de 90 días.
- Pruebas periódicas de restauración.
- Plan de continuidad documentado con escenarios de fallo de infraestructura, proveedores SMS y pasarela de pagos.
- Alternativas activas: Sibell mantiene capacidad multi-proveedor SMS para mitigar dependencia de un solo operador.
- Almacenamiento de copias en regiones distintas dentro de GCP.

---

10. Contacto y Procedimiento de Onboarding

10.1 Contactos

Asunto	Correo
Comercial	contacto@sibell.in
Soporte técnico	soporte@sibell.in
Privacidad y protección de datos	privacidad@sibell.in
Asuntos legales y contractuales	legal@sibell.in
Seguridad e incidentes	privacidad@sibell.in

10.2 Onboarding típico

1. **Sesión de descubrimiento** (30 min): caso de uso, volúmenes esperados, requerimientos de cumplimiento.
2. **Envío de paquete documental:** este Pack + DPA + propuesta comercial.
3. **Firma del DPA** y aceptación de los Términos del Servicio.
4. **Aprovisionamiento de cuenta y API Key**.
5. **Período de pruebas** en sandbox / Trial (100 SMS gratuitos).
6. **Paso a producción** con monitoreo conjunto los primeros 30 días.

---

11. Anexos y Referencias

- **Política de Tratamiento de Datos:** https://sibell.in/privacidad
- **Términos y Condiciones:** https://sibell.in/terminos
- **Documentación técnica (OpenAPI):** disponible bajo solicitud
- **Guía de integración con ejemplos en cURL, JavaScript, Python, Go, PHP:** disponible bajo solicitud
- **Catálogo de errores y matriz de reintentos:** disponible bajo solicitud
- **Marco normativo aplicable:**
- Constitución Política de Colombia, artículo 15
- Ley 1581 de 2012 (Habeas Data)
- Decreto 1377 de 2013
- Decreto 1074 de 2015 (DURP del sector Comercio)
- Ley 527 de 1999 (mensajes de datos y firma digital)
- Ley 1480 de 2011 (Estatuto del Consumidor)

Sibell SAS — NIT 901.916.609-5 — Bogotá D.C., Colombia

Confianza en cada verificación.