1) Política de Privacidad y Protección de Datos Personales Telemática Business Company S.A.

POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES
Versión: 1.0.0 — **Fecha de vigencia:** Entero 2026 - Diciembre 2026

1. Identidad del responsable del tratamiento

El responsable del tratamiento de tus datos personales es:

- **Razón social:** *Telemática Business Company S.A.*

- **Domicilio:** Whymper y Diego de Almagro
- **Ciudad / País:** Quito, Ecuador

- **Correo de privacidad:** desarrollo@tebusco.com.ec
- **Teléfono:** +593 9837281

- **Delegado de Protección de Datos :** Daniel Ruales | druales@tebusco.com.ec

(En adelante, el "**Responsable**"). La autoridad de control en Ecuador es la **Superintendencia de Protección de Datos Personales (SPDP)**.

2. Alcance

Esta política aplica al tratamiento de datos personales que realizamos a través de:

- El sitio web o sistemas informáticos en los siguientes dominios: tebusco.com.ec, grow.ec , tbo.com.ec

- Formularios (contacto, cotización, reclamos, postulación),

- Canales digitales integrados (chat, WhatsApp, CRM),

- Cookies y tecnologías similares.

3. Definiciones básicas

- **Titular:** persona natural a la que pertenecen los datos.

- **Responsable:** quien decide sobre finalidades y medios del tratamiento.
- **Encargado:** tercero que trata datos por cuenta del responsable (p. ej., hosting, CRM, email marketing).

4. Datos que recopilamos

Según el uso del sitio, podríamos tratar:

- **Identificación y contacto:** nombres, apellidos, correo, teléfono, empresa/cargo.
- **Datos de navegación:** IP, identificadores en línea, tipo de dispositivo, sistema operativo, eventos de navegación (cookies).
- **Contenido enviado por el usuario:** mensajes, adjuntos, solicitudes.
- **Preferencias comerciales/marketing:** intereses, historial de interacción.

No solicitamos datos sensibles (ni de salud, ni biométricos, etc.) a través del sitio, salvo que el servicio lo requiera y se gestione con medidas reforzadas y base de legitimación aplicable.

5. Finalidades del tratamiento

Tratamos tus datos para:

1. **Atender solicitudes** (contacto, cotizaciones, soporte).
2. **Gestionar relaciones comerciales y contractuales** (precontrato/contrato, facturación si aplica).
3. **Mejorar el sitio y la experiencia** (analítica, rendimiento, seguridad).
4. **Marketing y prospección** (newsletter, campañas) cuando lo autorices o cuando aplique una base legal válida con opción de oposición.
5. **Cumplimientos legales** y atención de requerimientos de autoridad competente.

6. Base de legitimación (LOPDP)

Tratamos datos cuando exista una condición de legitimidad, por ejemplo:

- **Consentimiento** del titular (libre, específico, informado e inequívoco y revocable).
- **Ejecución de medidas precontractuales o contractuales**.
- **Cumplimiento de obligación legal** u orden judicial.
- **Interés legítimo** del responsable o un tercero, cuando no prevalezcan los derechos del titular (p. ej., seguridad del sitio, prevención de fraude), aplicando evaluación de proporcionalidad.

Marketing directo: puedes **oponerte en cualquier momento** cuando el tratamiento tenga por objeto mercadotecnia directa, incluida la elaboración de perfiles para ese fin.

7. Conservación de los datos

Conservamos los datos **solo por el tiempo estrictamente necesario** para cumplir finalidades y obligaciones aplicables; luego procedemos a **eliminación, bloqueo o anonimización** según corresponda.

Criterio práctico sugerido (ajustable):

- Formularios de contacto/cotización: [12–24] meses.
- Leads/CRM sin contrato: [12–36] meses o hasta oposición/baja.
- Datos contractuales: el plazo que exija normativa tributaria/contractual aplicable.
- Logs de seguridad: [3–12] meses.

8. Destinatarios / encargados y transferencias

Podemos compartir datos con **encargados** que prestan servicios necesarios (p. ej., hosting, correo transaccional, CRM, analítica, mensajería), bajo obligaciones de confidencialidad y seguridad, y **solo para las finalidades descritas**.

Si existen **transferencias nacionales o internacionales**, se gestionarán conforme la LOPDP y normativa aplicable, documentando garantías/contratos y limitando accesos.

9. Seguridad de la información

Aplicamos medidas técnicas y organizativas apropiadas considerando **estado de la técnica, costos, naturaleza y riesgos** del tratamiento (p. ej., control de accesos, cifrado en tránsito, copias de seguridad, registros, mínimos privilegios, hardening).

10. Derechos del titular y cómo ejercerlos

Como titular puedes ejercer, entre otros:

- **Acceso** (conocer y obtener tus datos).
- **Rectificación y actualización**.
- **Eliminación** (cuando aplique).
- **Oposición** (incl. marketing directo).
- **Portabilidad** (recibir/transmitir datos en formato interoperable, cuando proceda).
- **Suspensión/limitación del tratamiento** en supuestos previstos.
- **No ser objeto de decisiones automatizadas** que produzcan efectos jurídicos o afecten derechos.

Canales para solicitar derechos:
Escríbenos a **desarrollo@tebusco.com.ec** con asunto “Derechos Datos Personales”. Habilitaremos canales informáticos simples y accesibles, sin perjuicio de medios físicos.

Plazos: Como referencia, la ley contempla atención de solicitudes (p. ej., acceso) dentro de **15 días** en varios supuestos.

Si no estás conforme con la respuesta, puedes acudir a la **SPDP** para presentar un reclamo.

11. Datos de niñas, niños y adolescentes

Si el sitio llegara a tratar datos de menores, se aplicarán reglas reforzadas. Los adolescentes desde **15 años** pueden otorgar consentimiento explícito en los términos previstos por la ley.

12. Cookies y tecnologías similares

Usamos cookies/SDKs para: (i) funcionamiento, (ii) analítica, (iii) marketing (si aplica). Podrás **configurar/aceptar/rechazar** cookies no esenciales desde [banner / centro de preferencias]. Para marketing, procuraremos consentimiento cuando corresponda.

13. Cambios a esta política

Podemos actualizar esta política para reflejar cambios legales o técnicos. Publicaremos la versión vigente y su fecha.

2) Política interna de manejo de datos personales (para el equipo de desarrollo y operación)

POLÍTICA INTERNA DE MANEJO DE DATOS PERSONALES
Versión: 1.0.0 — **Vigencia:** Enero 2026 - Diciembre 2026 — **Aprobación:** [Gerencia]

1. Objetivo

Establecer reglas y controles para el tratamiento de datos personales en el desarrollo, operación y soporte del sitio, garantizando cumplimiento de LOPDP y su Reglamento.

2. Roles y responsabilidades

- **Responsable del tratamiento:Telemática Business Company S.A.**
- **Encargados:** proveedores (hosting, CRM, analítica, mensajería).
- **Equipo interno (desarrollo/soporte):** actúa bajo instrucciones del responsable, con accesos mínimos y trazabilidad.

Recomendación contractual: dejar explícito **quién es Responsable** y quién es **Encargado** en el contrato del proyecto + anexos.

3. Principios operativos (checklist)

Todo tratamiento debe alinearse a:

- Finalidad clara y comunicada.
- Minimización (solo lo necesario).
- Seguridad y confidencialidad.
- Conservación limitada y eliminación segura.

4. Inventario y registro de tratamientos

Mantener un **inventario** por cada formulario/integración que incluya:

- Finalidad,

- Categorías de datos,
- Base de legitimación,
- Flujo (origen → destino),
- Encargados involucrados,
- Plazo de conservación,
- Medidas de seguridad.

(Esto facilita auditorías y respuesta a incidentes).

5. Gestión de accesos y ambientes

- Accesos por rol (mínimo privilegio).
- MFA obligatorio en paneles (hosting, CMS, CRM).
- Ambientes separados: DEV/QA/PROD.
- Prohibido usar datos reales en DEV; usar datos sintéticos/anonimizados cuando sea posible.

6. Desarrollo seguro y “privacidad desde el diseño”

En diseño y desarrollo:

- Validar que cada dato recolectado tenga finalidad + base legal.
- Formularios: campos mínimos, consentimiento donde aplique, logs de consentimiento.
- Cifrado TLS, hardening, WAF si aplica, backups con retención definida.
- Monitoreo de cambios y auditoría de accesos.

7. Conservación, eliminación y anonimización

- Definir plazos por cada conjunto de datos.

- Ejecutar **revisión periódica** y eliminación/bloqueo/anonimización cuando se cumpla la finalidad o plazo.

8. Atención de derechos (procedimiento interno mínimo)

1. Recepción por canal oficial (correo/formulario).
2. Verificación de identidad/representación.
3. Registro del caso (ticket) y trazabilidad.
4. Identificar sistemas afectados (web, CRM, backups).
5. Ejecutar acción (acceso/rectificación/eliminación/portabilidad/suspensión).
6. Responder dentro de plazos y dejar evidencia.

9. Evaluación de impacto (EIPD) cuando aplique

Antes de iniciar tratamientos de alto riesgo (p. ej., gran escala de categorías especiales, observación sistemática a gran escala), realizar **Evaluación de Impacto** previa y documentada.

10. Proveedores (encargados) y contratos

- Todo proveedor que trate datos debe firmar cláusulas de protección de datos (confidencialidad, seguridad, subencargados, apoyo en derechos, incidentes, eliminación al terminar).
- La SPDP ha publicado resoluciones relacionadas con obligaciones/estándares (por ejemplo, sobre incorporación de cláusulas en contratos).

11. Gestión de incidentes

- Definir un canal interno de incidentes (ticket).
- Contención, análisis, evidencias, corrección y lecciones aprendidas.
- Notificar a responsables/encargados y aplicar el procedimiento conforme marco local y contractual.

12. Capacitación y cumplimiento

- Inducción anual en privacidad y seguridad para personal con acceso a datos.
- Auditorías internas (semestrales / anuales) de accesos, plugins, integraciones y backups.

---

3) Anexo – Cláusula corta sugerida para el footer/formularios

“Al enviar este formulario, confirmas que has leído nuestra Política de Privacidad y aceptas el tratamiento de tus datos para atender tu solicitud.”

(Agregar checkbox cuando la base sea consentimiento, especialmente para marketing/newsletter).