DAPSITE (We Are Data Lab S.A.S.)

Términos de Servicio, Política de Uso Aceptable y Acuerdo de Soporte (EE. UU. y Colombia)

Última actualización: 30-09-2025

1) Definiciones clave

“DAPSITE” o **“Proveedor”**: We Are Data Lab S.A.S. y/o sus afiliados y subcontratistas.

“Cliente”: persona natural o jurídica que contrata los Servicios.

“Servicios”: mantenimiento, soporte, administración, optimización, monitoreo y tareas de contenido para sitios web (inicialmente WordPress), según el plan vigente y/o documentos de alcance.

“Cambio básico”: solicitud que **no requiere** diseño gráfico con mockups, **no implica** integraciones ni desarrollo a medida y **no supera 2 horas** de ejecución total.

“Incidente de seguridad”: hackeo, malware, explotación de vulnerabilidades, caída severa de servicio o pérdida de datos.

“Elementos de terceros”: hosting, dominios, certificados SSL, temas, plugins, librerías, pasarelas, analítica, CDNs, etc., proporcionados por terceros.

“Plataforma”: sistema de tickets y panel de Cliente donde se registran solicitudes, reportes y comunicaciones.

2) Alcance del servicio por plan (resumen)

- **Actualizaciones periódicas** de núcleo, temas y plugins; **monitoreo 24/7** de uptime; **backups automáticos**; **firewall/antimalware**; **optimización de rendimiento**; **reportes** y **soporte** según plan.

- **Cambios básicos de contenido ilimitados**, gestionados **uno a la vez** por orden de llegada. Quedan **excluidas** tareas que requieran diseño complejo, integraciones, desarrollo o que excedan 2 horas. Esas tareas se cotizan por fuera o se rechazan.

- **Limpieza de hackeos** y **restauración** desde backups cuando el plan contratado lo incluye.

- La **promesa específica** (p. ej., Core Web Vitals “Bueno”) **solo aplica** si está expresamente pactada en el plan o anexo.

Los detalles exactos de cada plan (Básico, Estándar, Pro/multisitio) constan en la propuesta comercial y/o anexo de servicios y pueden actualizarse sin afectar derechos adquiridos durante el período prepagado.

3) Solicitudes y límites operativos

3.1. Ventanilla única. Todas las solicitudes deben radicarse en la Plataforma. Una sola solicitud activa por vez. Al completar una, iniciamos la siguiente.

3.2. Complejidad excedida. Nos reservamos el derecho de **rechazar** solicitudes que excedan el concepto de **Cambio básico** o que, a nuestra discreción técnica, comprometan estabilidad, seguridad o lineamientos de buenas prácticas. Alternativamente, podremos proponer **cotización** por fuera del plan.

3.3. Prioridad. Incidentes críticos (caída total, hackeo activo, pérdida de datos) se atienden con prioridad sobre cambios de contenido.

3.4. Ventanas de mantenimiento. Actualizaciones mayores pueden ejecutarse en ventanas programadas (horario no pico) para mitigar riesgo.

4) Seguridad, vulnerabilidades y responsabilidades

4.1. Naturaleza del riesgo. En WordPress, gran parte del riesgo proviene de **plugins y temas de terceros**. El Proveedor **no garantiza** ausencia total de vulnerabilidades.

4.2. Prácticas del Proveedor. Aplicamos parches de seguridad, escaneos, firewall, endurecimiento, revisión de dependencias y monitoreo. Cuando se detecten vulnerabilidades críticas, podremos **desactivar** temporalmente componentes de terceros para proteger el sitio.

4.3. Responsabilidades del Cliente. (i) Mantener **contraseñas fuertes** y 2FA en los accesos bajo su control (hosting, correos, CDN, pasarelas, etc.). (ii) **No** instalar plugins/temas sin validación del Proveedor durante la vigencia del servicio. (iii) Proveer accesos **administrativos** y **actualizados** al inicio del servicio.

4.4. Incidentes de seguridad. Si se presenta un incidente: (i) **Contención** (aislamiento, bloqueo, desactivación de componentes comprometidos), (ii) **Remediación** (limpieza de malware, parcheo, hardening), (iii) **Restauración** (desde backups válidos), (iv) **Lecciones aprendidas** (recomendaciones). Si el plan no incluye limpieza de hackeos o la causa se originó por acciones del Cliente o terceros no autorizados, los costos de remediación **serán facturados**.

4.5. Contenidos y datos. El Cliente es titular de sus contenidos/datos y es responsable de su licitud. El Proveedor no es responsable por pérdidas cuando la causa sea ajena a su

control (hosting, proveedor de correo, registrar, CDN, fallas generalizadas de la nube, caso fortuito/ fuerza mayor, acciones de terceros, errores del Cliente, etc.).

5) Backups y restauración

5.1. Cobertura. Hacemos backups automáticos conforme al plan; sin embargo, por su naturaleza, **ningún backup es infalible**.

5.2. Copias del Cliente. El Cliente **debe** mantener **copias externas** adicionales. A solicitud, podemos entregar snapshots disponibles. No somos responsables por pérdidas si el último backup íntegro no contiene la versión exacta deseada.

5.3. RPO/RTO. Objetivos de punto y tiempo de recuperación son **esfuerzos razonables**; dependerán del tamaño del sitio, del hosting, del tráfico y de la salud de la base de datos.

6) Uso Aceptable (AUP)

6.1. Prohibiciones. Queda prohibido: (i) malware, phishing, spam masivo, botnets, ataques (DDoS, fuerza bruta, escaneo de puertos), (ii) contenido ilícito (p. ej., pornografía infantil), (iii) infracción de derechos de autor o marcas, (iv) distribución de software ilegal o evasión de seguridad, (v) cualquier uso contrario a la ley aplicable en EE. UU. o Colombia.

6.2. Cumplimiento y suspensión. El Proveedor podrá **suspender** total o parcialmente los Servicios ante violaciones al AUP, incidentes graves o requerimientos legales. En casos graves o de reincidencia, podrá **terminar** el servicio sin reembolso del periodo en curso.

6.3. Correo y marketing. Queda prohibido el **spam** y el uso de la infraestructura para campañas no autorizadas. Podrán aplicarse **cargos de limpieza** y costos de terceros por abuso.

7) Exclusiones frecuentes

- Desarrollo a medida, integraciones, comercio electrónico avanzado, rediseños completos, branding, edición de video, fotografía, ilustración, copywriting estratégico, SEO gestionado, campañas de ads, migraciones complejas y auditorías legales o de cumplimiento (salvo pacto expreso).

- Tareas que superen las **2 horas** de ejecución o requieran diseño con **mockups**.

- Reparaciones o refactors causados por **intervenciones de terceros** o por el propio Cliente fuera del flujo de trabajo acordado.

- Garantías de **uptime**, **posicionamiento SEO**, resultados de negocio o métricas específicas, salvo compromiso **explícito** por escrito.

8) Niveles de servicio y tiempos de respuesta (SLA)

8.1. Prioridades. Crítico (sitio caído, hackeo activo): mejor esfuerzo inmediato. Alto (fallo funcional severo): primeras 4–24 h hábiles. Medio/Bajo (cambios de contenido, ajustes menores): cola estándar.

8.2. Ventanas y coordinación. Cambios con impacto en UX o embudos de venta pueden programarse para minimizar disrupción.

8.3. Reportería. En planes aplicables, entregamos reportes mensuales de actualizaciones, estado, rendimiento y seguridad.

9) Precios, facturación y renovaciones

9.1. Prepago. Todos los planes son **prepagados** por periodos mensuales o anuales. La renovación es **automática** hasta cancelación.

9.2. Cambios de precio. Podemos ajustar precios, informando antes de su vigencia. Cambios no aplican retroactivamente a periodos ya pagados.

9.3. Reembolsos. No hay reembolsos por periodos ya iniciados ni por meses parcialmente usados. Cancelaciones aplican al periodo siguiente.

9.4. Moras. Falta de pago podrá conllevar **suspensión** y/o **terminación** del servicio, con eliminación de accesos y licencias temporales (p. ej., plugins premium provistos por el Proveedor).

10) Propiedad intelectual

10.1. Del Cliente. El Cliente conserva la titularidad de sus contenidos y marcas. Es responsable de contar con todas las licencias y permisos.

10.2. Del Proveedor. El Proveedor conserva derechos sobre herramientas, scripts, configuraciones y know-how. Puede licenciar **plugins premium** para uso durante la vigencia del plan; al terminar, el Cliente deberá adquirir sus propias licencias o aceptar la desactivación.

11) Confidencialidad y acceso

11.1. Accesos. El Cliente facilitará accesos administrativos necesarios (hosting, panel, CMS, DNS, CDN) y mantendrá actualizada la lista de contactos autorizados.

11.2. Confidencialidad. Cada parte se obliga a proteger la información confidencial de la otra y a usarla solo para la ejecución del servicio.

11.3. No solicitación. Durante el servicio y por **12 meses** posteriores, el Cliente se abstendrá de contratar directamente al personal/contratistas del Proveedor involucrados en

la prestación (salvo acuerdo escrito). Penalidad: **12 meses** de la compensación anual de la persona involucrada o lo que dispongan las leyes aplicables.

12) Garantías, descargos y limitación de responsabilidad

12.1. "Tal cual". En la medida permitida por la ley, los Servicios se prestan **"AS IS / TAL CUAL"**, sin garantías implícitas de comerciabilidad, idoneidad para un propósito particular o no infracción.

12.2. No indemnizamos. El Proveedor **no otorga indemnización** al Cliente por reclamaciones de terceros. El Cliente **sí** se compromete a **defender, indemnizar y mantener indemne** al Proveedor frente a reclamaciones derivadas de (i) contenidos del Cliente, (ii) uso indebido, (iii) violaciones al AUP, (iv) incumplimiento contractual del Cliente, (v) infracción de derechos de terceros por parte del Cliente.

12.3. Límite de responsabilidad. La responsabilidad total agregada del Proveedor por cualquier reclamo se limita al **monto efectivamente pagado por el Cliente** por el servicio que dio lugar al reclamo, ya sea el **último periodo facturado** o, a elección del Proveedor, la suma pagada en los **últimos 3 meses**, lo que sea **menor**. En ningún caso respondemos por **lucro cesante**, pérdida de datos, daño reputacional, interrupción de negocio, costos de sustitución, ni daños indirectos, especiales, emergentes o punitivos.

12.4. Fuerza mayor. Ninguna parte será responsable por incumplimientos debidos a causas fuera de su control razonable (desastres naturales, cortes generalizados de nube/infraestructura, guerra, embargos, fallas de proveedores críticos, actos gubernamentales, huelgas, etc.).

13) Entrada en vigor, suspensión y terminación

13.1. Inicio. El servicio inicia tras confirmación de pago y entrega de accesos.

13.2. Suspensión. Podemos suspender por (i) mora, (ii) incidentes graves de seguridad, (iii) violación al AUP o a la ley, (iv) riesgos inminentes para la infraestructura.

13.3. Terminación. Cualquiera de las partes puede terminar con aviso previo conforme al ciclo de facturación. Las obligaciones que por su naturaleza deban subsistir (propiedad intelectual, confidencialidad, no solicitación, limitación de responsabilidad, ley aplicable) **sobreviven**.

14) Ley aplicable y jurisdicción

Clientes en Colombia: Este Acuerdo se rige por las leyes de **Colombia**. Jurisdicción: **Jueces de Bogotá D.C.**

Clientes en EE. UU.: Este Acuerdo se rige por las leyes del **Estado de [elegir: Florida / Texas / Delaware]**, sin conflicto de leyes. Jurisdicción y sede: **[Condado y Estado elegidos]**. Alternativamente, las partes pueden pactar **arbitraje** comercial administrado por **AAA** en inglés.

15) Cambios a estos Términos

Podemos actualizar estos Términos y publicarlos en la Plataforma o sitio. El uso continuado implica aceptación. Notificaremos cambios materiales con antelación razonable.

16) Privacidad y datos personales (sin UE)

Tratamos datos personales conforme a leyes aplicables de **EE. UU. y Colombia**. No incorporamos obligaciones del **GDPR** ni otras normas de la **Unión Europea**. Para clientes con audiencia en la UE, la **conformidad normativa** deberá contratarse como servicio **separado**.

17) Contacto

Soporte y legal: [tu correo] | **Dirección:** [tu dirección empresarial]

Anexo A — Ejemplos de Cambios Básicos (orientativos)

- Crear/editar entradas de blog, páginas informativas, textos y medios ya proporcionados por el Cliente.
- Ajustes menores de CSS, márgenes, tipografías y colores existentes.
- Reemplazo de imágenes, optimización simple de peso y formatos.
- Inserción de códigos de seguimiento (Analytics, Pixel), verificación Search Console.
- Configuraciones simples en plugins existentes (sin nuevas integraciones).

No son básicos: maquetación completa de nuevas secciones, rediseños, funnels complejos, integraciones con APIs, e-commerce, funcionalidades a medida, migraciones de hosting, multi-idioma completo, desarrollo de temas/child a medida, ni tareas > 2 horas.

Anexo B — Flujo ante Incidente de Seguridad

1. **Detección** (alerta/monitor) → 2. **Contención** (bloquear IPs, desactivar plugins comprometidos, modo mantenimiento) → 3. **Remediación** (limpieza malware, parches, hardening) → 4. **Restauración** (backup/snapshot) → 5. **Verificación** (escaneo final) → 6. **Informe** → 7. **Recomendaciones** (actualizaciones, sustitución

de plugins abandonados, 2FA, rotación de claves).

Nota final: Este documento es modular y puede adaptarse a acuerdos marco, órdenes de servicio y anexos técnicos por cliente. Sustituye versiones anteriores.