

ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN

NDA / Non-Disclosure Agreement

En la ciudad de _____, República del Paraguay, a los ____ días del mes de _____ de 20, comparecen:

Por una parte, _____, con RUC / documento N.º _____, con domicilio en _____, representada por _____, en adelante “el Cliente”;

y por otra parte, _____, con RUC N.º _____, con domicilio en _____, en adelante “el Prestador”;

quienes conjuntamente serán denominados “las Partes”, y acuerdan celebrar el presente **Acuerdo de Confidencialidad y No Divulgación**, en adelante “el Acuerdo”, conforme a las siguientes cláusulas:

1. Objeto del Acuerdo

1.1. El presente Acuerdo tiene por objeto regular la entrega, uso, custodia, protección y no divulgación de la información confidencial a la que cualquiera de las Partes pueda tener acceso con motivo de la negociación, contratación, ejecución o finalización de servicios de tecnología, desarrollo de software, integración, configuración, soporte, administración de servidores, auditoría técnica, DevOps, automatización, inteligencia artificial u otros servicios relacionados.

1.2. El presente Acuerdo complementa el contrato principal de prestación de servicios, la propuesta comercial, la orden de trabajo, la especificación técnica y cualquier otro documento acordado entre las Partes.

1.3. La finalidad del Acuerdo es proteger la información comercial, técnica, operativa, financiera, legal y estratégica de las Partes, así como los datos, accesos, sistemas, infraestructura y documentación vinculados al proyecto.

2. Información Confidencial

2.1. Se entenderá por **Información Confidencial** toda información entregada, revelada, comunicada o puesta a disposición por una Parte a la otra, en forma escrita, oral, electrónica, visual, técnica, documental o por cualquier otro medio, incluyendo, sin limitarse a:

- a) código fuente, scripts, librerías, configuraciones y repositorios;
- b) bases de datos, estructuras de tablas, volcados, respaldos, logs y reportes;

- c) contraseñas, tokens, claves API, claves SSH, certificados, credenciales y secretos técnicos;
- d) información sobre servidores, dominios, hosting, infraestructura cloud, redes, VPN, firewalls y sistemas internos;
- e) datos de clientes, usuarios, empleados, proveedores, contratistas y socios comerciales;
- f) información financiera, precios, tarifas, costos, márgenes, presupuestos y condiciones comerciales;
- g) procesos internos, metodologías, estrategias, manuales, políticas y procedimientos;
- h) documentación técnica, especificaciones, diagramas, tickets, tareas, mensajes y correspondencia del proyecto;
- i) información sobre incidentes, vulnerabilidades, auditorías, configuraciones de seguridad o riesgos técnicos;
- j) cualquier información marcada como confidencial, reservada o privada;
- k) cualquier información que, por su naturaleza o contexto, razonablemente deba entenderse como no destinada a divulgación pública.

2.2. También será considerada Información Confidencial toda información a la que el Prestador acceda dentro de sistemas, servidores, bases de datos, repositorios, paneles administrativos, herramientas internas o entornos técnicos del Cliente, aunque dicha información no esté expresamente marcada como confidencial.

2.3. Salvo autorización expresa y por escrito, también se considerará confidencial el hecho mismo de la relación comercial entre las Partes, el nombre del proyecto, la identidad del Cliente, el alcance de los servicios y los detalles de la infraestructura técnica del Cliente.

3. Obligaciones de confidencialidad

3.1. La Parte que reciba Información Confidencial se obliga a:

- a) utilizarla únicamente para los fines relacionados con el proyecto o servicio acordado;
- b) no divulgarla a terceros sin autorización previa y por escrito de la Parte reveladora;
- c) no publicarla en sitios web, redes sociales, portafolios, presentaciones, repositorios públicos, foros, comunidades técnicas o materiales comerciales;
- d) no copiarla, exportarla, conservarla ni reproducirla más allá de lo estrictamente necesario para la ejecución del servicio;
- e) aplicar medidas razonables de seguridad técnica y organizativa para protegerla;
- f) limitar el acceso a dicha información únicamente a las personas que deban conocerla para cumplir la tarea acordada;
- g) informar a la otra Parte en caso de sospecha razonable de filtración, pérdida, acceso no autorizado, compromiso de credenciales o uso indebido de la Información Confidencial.

3.2. El Prestador no podrá utilizar la Información Confidencial del Cliente para fines propios, comerciales, publicitarios, formativos, demostrativos, ni para proyectos de terceros, salvo autorización expresa y por escrito del Cliente.

3.3. El Cliente no podrá divulgar metodologías internas, plantillas, herramientas, documentación, know-how, propuestas técnicas o condiciones comerciales del Prestador si tales materiales fueron entregados como confidenciales o no destinados a distribución pública.

4. Exclusiones

4.1. No será considerada Información Confidencial aquella información que:

- a) fuera de dominio público al momento de su entrega;
- b) se vuelva pública sin incumplimiento de este Acuerdo por parte de la Parte receptora;
- c) haya sido obtenida legítimamente de un tercero sin obligación de confidencialidad;
- d) haya sido desarrollada de forma independiente por la Parte receptora sin utilizar Información Confidencial de la otra Parte;
- e) deba ser revelada por mandato legal, judicial, administrativo o por requerimiento de autoridad competente.

4.2. Si una Parte estuviera obligada a revelar Información Confidencial por requerimiento de una autoridad competente, deberá, en la medida legalmente permitida, notificar previamente a la otra Parte y limitar la revelación al mínimo necesario.

5. Accesos, credenciales y secretos técnicos

5.1. Las contraseñas, tokens, claves API, claves SSH, certificados, claves privadas, credenciales de paneles administrativos y demás secretos técnicos se consideran Información Confidencial de carácter especialmente sensible.

5.2. El Prestador se obliga a no incluir dichos secretos en:

- a) repositorios públicos;
- b) código fuente sin necesidad técnica justificada;
- c) archivos no protegidos;
- d) logs abiertos;
- e) volcados de prueba;
- f) capturas de pantalla;
- g) documentación accesible a terceros;
- h) herramientas externas de inteligencia artificial sin autorización previa.

5.3. El Cliente podrá revocar, modificar, rotar o cancelar en cualquier momento los accesos temporales concedidos al Prestador.

5.4. Al finalizar los trabajos, se recomienda al Cliente revocar accesos temporales, eliminar usuarios provisionales, cambiar contraseñas, regenerar tokens y revisar las claves activas.

6. Uso de herramientas de inteligencia artificial

6.1. El Prestador podrá utilizar herramientas de inteligencia artificial para acelerar el desarrollo, analizar arquitectura, preparar documentación, detectar errores, generar código auxiliar y mejorar la eficiencia técnica del proyecto.

6.2. Sin embargo, el Prestador no transmitirá a servicios externos de inteligencia artificial, sin autorización previa y por escrito del Cliente:

- a) bases de datos reales;
- b) datos personales;
- c) listas de clientes, usuarios o empleados;
- d) contraseñas, tokens, claves API, claves SSH o certificados;
- e) código fuente privado del Cliente;
- f) documentación técnica interna;
- g) información financiera o comercial sensible;
- h) información sobre vulnerabilidades, configuraciones de seguridad o infraestructura crítica.

6.3. Para el uso de herramientas de inteligencia artificial podrán emplearse ejemplos sintéticos, datos anonimizados, fragmentos sin secretos, descripciones generales de arquitectura o entornos locales/aislados, siempre que ello no permita identificar al Cliente, sus clientes, su infraestructura o su información confidencial.

7. Datos personales

7.1. Si durante la ejecución de los servicios el Prestador accede a datos personales de clientes, usuarios, empleados, proveedores o terceros vinculados al Cliente, dichos datos deberán ser tratados con medidas adicionales de protección y únicamente para los fines autorizados.

7.2. El Prestador se obliga a no copiar, extraer, almacenar, transferir, reutilizar ni tratar datos personales fuera del alcance necesario para la tarea acordada.

7.3. Cuando el proyecto implique tratamiento regular de datos personales, las Partes podrán suscribir un acuerdo específico de tratamiento de datos personales o incorporar cláusulas adicionales en el contrato principal, de conformidad con la normativa aplicable en la República del Paraguay.

7.4. Siempre que sea posible, para desarrollo, pruebas, depuración y demostraciones se utilizarán datos anonimizados, seudonimizados o sintéticos en lugar de datos personales reales.

8. Código fuente, documentación y resultados del trabajo

8.1. Los derechos sobre el código fuente, documentación, configuraciones, entregables y demás resultados del trabajo serán determinados por el contrato principal, propuesta comercial, orden de trabajo, factura, acta de entrega o acuerdo escrito entre las Partes.

8.2. Salvo pacto en contrario, el código fuente desarrollado específicamente para el Cliente y pagado por el Cliente podrá ser utilizado por el Cliente para la operación, mantenimiento, evolución y soporte del proyecto correspondiente.

8.3. El Prestador no podrá publicar, reutilizar, vender, transferir ni entregar a terceros el código fuente privado del Cliente sin autorización previa y por escrito.

8.4. El Prestador conserva sus derechos sobre metodologías generales, conocimientos previos, herramientas propias, plantillas, librerías, frameworks, componentes reutilizables y know-how preexistente, siempre que no contengan Información Confidencial del Cliente ni reproduzcan elementos específicos protegidos del proyecto.

9. Publicaciones, portafolio y referencias comerciales

9.1. El Prestador no podrá mencionar el nombre del Cliente, logotipo, capturas de pantalla, métricas, resultados, descripción del proyecto, arquitectura, documentación, enlaces internos ni ninguna referencia identificable en portafolios, redes sociales, páginas web, propuestas comerciales, presentaciones o materiales públicos sin autorización previa y por escrito del Cliente.

9.2. El Cliente podrá autorizar al Prestador a utilizar el proyecto como caso de éxito, referencia comercial o experiencia profesional. Dicha autorización deberá constar por escrito y podrá establecer límites sobre la información que puede divulgarse.

10. Plazo de vigencia

10.1. El presente Acuerdo entrará en vigencia a partir de la fecha de su firma por las Partes.

10.2. Las obligaciones de confidencialidad permanecerán vigentes durante toda la relación comercial entre las Partes y por un plazo de **cinco años** contados desde la finalización de la relación, salvo que el contrato principal establezca un plazo mayor.

10.3. Respecto de secretos técnicos, credenciales, claves, código fuente, bases de datos, información de seguridad, listas de clientes, know-how sensible y secretos comerciales, la obligación de confidencialidad permanecerá vigente por tiempo indefinido o hasta que dicha información se vuelva pública de forma lícita.

11. Devolución, eliminación o destrucción de información

11.1. A solicitud de la Parte reveladora, la Parte receptora deberá devolver, eliminar o destruir la Información Confidencial recibida, siempre que su conservación no sea necesaria para cumplir obligaciones legales, contables, fiscales, contractuales o para la defensa de derechos legítimos.

11.2. El Prestador podrá conservar una copia mínima de documentación administrativa o evidencias de trabajo necesarias para acreditar la prestación del servicio, facturación, cumplimiento tributario o defensa legal, siempre manteniendo la confidencialidad correspondiente.

11.3. La eliminación de accesos técnicos deberá coordinarse con el Cliente, quien será responsable de revocar usuarios, claves, tokens y permisos dentro de sus propios sistemas cuando corresponda.

12. Incidentes de seguridad

12.1. Si cualquiera de las Partes detecta una sospecha razonable de filtración, pérdida, acceso no autorizado, publicación accidental, compromiso de credenciales o uso indebido de Información Confidencial, deberá notificar a la otra Parte en un plazo razonable.

12.2. La notificación deberá incluir, en la medida de lo posible, la siguiente información:

- a) naturaleza del incidente;
- b) fecha o momento estimado de detección;
- c) tipo de información potencialmente afectada;
- d) medidas adoptadas inicialmente;
- e) recomendaciones para mitigar el impacto;
- f) acciones pendientes o necesarias.

12.3. Las Partes se comprometen a colaborar de buena fe para contener el incidente, reducir sus consecuencias y evitar su repetición.

13. Responsabilidad

13.1. La Parte que incumpla el presente Acuerdo será responsable por los daños directos, ciertos y documentados que dicho incumplimiento cause a la otra Parte, conforme al derecho aplicable.

13.2. Las Partes podrán establecer una penalidad contractual por incumplimiento de confidencialidad en el monto de: _____.

13.3. El pago de una penalidad no libera a la Parte infractora de la obligación de cesar la conducta indebida, eliminar la información divulgada indebidamente y adoptar medidas razonables para reducir los daños.

13.4. Ninguna de las Partes será responsable por una divulgación que ocurra por causa no imputable, fuerza mayor, hecho de tercero, requerimiento legal obligatorio o incidente que no hubiera podido evitarse mediante medidas razonables de protección.

14. Notificaciones

14.1. Las notificaciones relacionadas con el presente Acuerdo podrán realizarse por escrito, correo electrónico, documento electrónico, mensajería empresarial acordada o cualquier otro medio que permita acreditar razonablemente su envío y recepción.

14.2. A efectos de notificaciones, las Partes declaran como correos electrónicos válidos:

Cliente: _____

Prestador: _____

14.3. Cada Parte deberá informar oportunamente cualquier cambio de domicilio, correo electrónico o datos de contacto.

15. Ley aplicable y jurisdicción

15.1. El presente Acuerdo se registrará e interpretará conforme a las leyes de la República del Paraguay.

15.2. Las Partes procurarán resolver de buena fe cualquier controversia mediante negociación directa.

15.3. Si la controversia no pudiera resolverse mediante negociación, será sometida a los tribunales competentes de la República del Paraguay, en la ciudad de _____, salvo que las Partes acuerden expresamente otro mecanismo de resolución de disputas.

16. Firma electrónica y documentos digitales

16.1. Las Partes reconocen que el presente Acuerdo podrá ser firmado en formato físico, mediante intercambio de copias escaneadas, documentos electrónicos, firma electrónica, firma digital u otro medio que permita acreditar razonablemente la aceptación de las Partes, siempre que ello no contradiga la legislación aplicable.

16.2. Los documentos, mensajes, correos electrónicos, anexos, propuestas y aceptaciones intercambiados por medios electrónicos podrán ser utilizados como evidencia de la relación contractual, del alcance de los trabajos y de las obligaciones asumidas por las Partes.

17. Disposiciones finales

17.1. El presente Acuerdo constituye el entendimiento completo de las Partes respecto de la confidencialidad de la información, sin perjuicio de lo establecido en el contrato principal u otros documentos complementarios.

17.2. Cualquier modificación al presente Acuerdo deberá realizarse por escrito y contar con la aceptación de ambas Partes.

17.3. La nulidad o invalidez de una cláusula no afectará la validez de las demás disposiciones del Acuerdo.

17.4. El presente Acuerdo se firma en dos ejemplares de igual tenor y efecto, uno para cada Parte, o en formato electrónico aceptado por ambas Partes.

18. Datos y firmas de las Partes

EL CLIENTE

Nombre / Razón social: _____

RUC / Documento N.º: _____

Domicilio: _____

Representante: _____

Cargo: _____

Correo electrónico: _____

Firma: _____

Fecha: ____ / ____ / 20____

EL PRESTADOR

Nombre / Razón social: _____

RUC N.º: _____

Domicilio: _____

Correo electrónico: _____

Teléfono: _____

Firma: _____

Fecha: ____ / ____ / 20____
