REGLAMENTO
PARA LA PRESTACIÓN SEGURA DE SERVICIOS IT

Y PROTECCIÓN DE LA INFORMACIÓN CONFIDENCIAL DEL CLIENTE

El presente reglamento describe los principios organizativos y técnicos que el Prestador aplica al prestar servicios de desarrollo, integración, configuración y soporte de software.

Este documento complementa el contrato de prestación de servicios y el acuerdo de confidencialidad. Su objetivo es proporcionar al Cliente una comprensión clara de cómo el Prestador reduce los riesgos de fuga de información comercial, acceso no autorizado a datos, incorporación de código no verificado y compromiso de la infraestructura del Cliente.

El presente reglamento no constituye una promesa de protección absoluta ni de “riesgo cero”, ya que en materia de seguridad de la información tales garantías no son posibles. En su lugar, el Prestador aplica medidas verificables de control, limitación de accesos, aislamiento de entornos de trabajo y entrega transparente de los resultados.

---

1. Estatus del Prestador y responsabilidad

El Prestador presta sus servicios dentro del marco legal de la República del Paraguay, utilizando su número oficial de identificación tributaria RUC.

Los trabajos se realizan sobre la base de un contrato, una especificación técnica, la correspondencia con el Cliente y un acuerdo de confidencialidad.

El Prestador se obliga a no divulgar a terceros información relacionada con los procesos de negocio, infraestructura, clientes, bases de datos, código fuente, información financiera, arquitectura técnica u otros materiales del Cliente obtenidos durante la ejecución de los trabajos.

La información sobre los proyectos del Cliente no se publica en portafolios, materiales publicitarios, redes sociales, repositorios públicos o presentaciones sin el consentimiento previo y por escrito del Cliente.

---

2. Principio de acceso mínimo

El Prestador no solicita acceso completo a la infraestructura del Cliente si ello no es necesario para cumplir una tarea concreta.

El acceso se concede únicamente a los sistemas, módulos, API, repositorios o entornos de prueba directamente relacionados con los trabajos en curso.

Siempre que sea posible, se aplica el principio de Need-to-Know: el Prestador recibe únicamente la información y los permisos necesarios para la etapa actual del proyecto.

El acceso a servidores de producción, bases de datos operativas y sistemas que contengan datos reales de clientes no se utiliza salvo necesidad justificada y previo acuerdo específico con el Cliente.

---

3. Aislamiento de entornos de trabajo

El desarrollo, las pruebas y la depuración se realizan en un entorno de trabajo aislado, separado de la infraestructura de producción del Cliente.

Como entornos de trabajo pueden utilizarse servidores VPS independientes, entornos de prueba, servidores staging, contenedores locales u otras plataformas técnicas aisladas.

El Prestador no realiza experimentos, depuración ni verificación inicial de código directamente en los servidores de producción del Cliente, salvo acuerdo específico en contrario.

El objetivo de este enfoque es evitar que un error durante el desarrollo pueda afectar datos reales, clientes o la estabilidad del servicio en funcionamiento.

---

4. Trabajo con bases de datos e información comercial

Para el desarrollo y las pruebas, el Prestador no requiere bases de datos reales del Cliente si la tarea puede ejecutarse con datos anonimizados o sintéticos.

Se recomienda al Cliente proporcionar estructuras de tablas, esquemas de datos, volcados de prueba, muestras anonimizadas o datos generados artificialmente en lugar de bases reales.

Si para la ejecución de una tarea fuera necesario analizar datos reales, dicho acceso deberá acordarse por separado. En tal caso, el volumen de datos deberá limitarse al mínimo necesario.

El Prestador no copia, almacena ni utiliza datos reales del Cliente fuera del marco de la tarea acordada.

---

5. Uso de herramientas de inteligencia artificial

El Prestador puede utilizar herramientas de inteligencia artificial para acelerar el desarrollo, analizar arquitectura, preparar documentación, detectar errores y generar código auxiliar.

No obstante, los datos confidenciales del Cliente no se transmiten a servicios externos de inteligencia artificial sin acuerdo previo.

Se consideran datos confidenciales: bases de datos reales, contraseñas, tokens, claves API, certificados privados, listas de clientes, información financiera, condiciones comerciales, código fuente cerrado y documentación técnica interna.

Para trabajar con herramientas de inteligencia artificial se utilizan fragmentos anonimizados, ejemplos sintéticos, descripciones arquitectónicas sin secretos o entornos locales/aislados, si el proyecto así lo requiere.

---

6. Gestión de accesos y secretos

Las contraseñas, tokens, claves SSH, claves API y otros secretos deben transmitirse de forma segura y utilizarse únicamente para los fines del proyecto.

El Prestador no almacena contraseñas ni claves en texto plano dentro del código fuente, repositorios públicos, documentación o archivos no protegidos.

Los secretos no deben incluirse en repositorios Git, registros de sistema, volcados de prueba, capturas de pantalla o correspondencia, siempre que ello pueda evitarse.

Al finalizar los trabajos, se recomienda al Cliente revocar los accesos temporales, cambiar las contraseñas entregadas, regenerar tokens y eliminar cuentas temporales.

---

7. Control del código fuente

Todos los cambios sustanciales del código fuente se entregan mediante un sistema de control de versiones, como GitLab, GitHub, Bitbucket u otro repositorio acordado.

El uso de Git permite registrar el historial de cambios, el autor de cada modificación, la fecha de modificación y el contenido del código entregado.

Según lo acordado con el Cliente, los cambios pueden entregarse mediante ramas separadas, merge requests / pull requests, archivos de release u otros mecanismos controlados.

El Cliente tiene derecho a revisar el código fuente antes de su implementación en el entorno de producción.

---

8. Releases e implementación de cambios

La implementación de cambios en el entorno de producción debe realizarse de forma controlada.

El procedimiento recomendado es el siguiente:

1. desarrollo en un entorno separado;
2. pruebas en entorno dev/staging;
3. revisión de los cambios por parte del Cliente o su especialista técnico;
4. preparación del release;
5. implementación en producción;
6. verificación del resultado después de la implementación.

La copia manual de archivos individuales al servidor de producción solo se permite como medida temporal o de emergencia, si no es posible utilizar un mecanismo automatizado de release.

La opción preferente es el uso de CI/CD, archivos de release, scripts de despliegue u otro mecanismo reproducible de entrega de código.

---

9. Acciones prohibidas

El Prestador tiene prohibido:

transmitir materiales del Cliente a terceros sin el consentimiento del Cliente;

publicar código fuente, documentación, esquemas, capturas de pantalla o información sobre el proyecto sin autorización;

utilizar datos reales del Cliente para pruebas cuando puedan utilizarse datos anonimizados o sintéticos;

incluir secretos, contraseñas o tokens en el código o en repositorios públicos;

copiar bases de datos de producción sin acuerdo previo;

utilizar los accesos del Cliente para tareas no relacionadas con el proyecto;

conservar accesos después de la finalización de los trabajos si el Cliente ha solicitado su eliminación o ha revocado dichos accesos.

---

10. Derecho del Cliente a auditoría

El Cliente tiene derecho a revisar el código fuente entregado, la documentación, las configuraciones y los materiales de release por sí mismo o con la participación de especialistas técnicos independientes.

El Prestador no obstaculizará dicha revisión dentro del alcance acordado de los trabajos y de los materiales entregados.

La auditoría puede realizarse antes de la implementación, después del release, durante la aceptación de una etapa de trabajo o al finalizar el proyecto.

---

11. Respuesta ante incidentes

Si el Prestador detecta una sospecha de fuga de datos, compromiso de claves, acceso no autorizado, publicación accidental de materiales u otro incidente de seguridad, notificará al Cliente en un plazo razonable.

Tras detectar un incidente, el Prestador adoptará medidas para limitar sus consecuencias: dejará de utilizar los accesos sospechosos, registrará las circunstancias, comunicará al Cliente los detalles conocidos y participará en la solución del problema dentro de su ámbito de responsabilidad.

Después de cualquier incidente, se recomienda al Cliente regenerar claves, cambiar contraseñas, revisar registros de acceso y limitar las cuentas temporales.

---

12. Finalización de los trabajos

Al finalizar el proyecto, una etapa de trabajo o el contrato, el Prestador entrega al Cliente los resultados acordados: código fuente, documentación, instrucciones de puesta en marcha, configuraciones, esquemas, materiales de release y otros artefactos previstos en el contrato o en la especificación técnica.

El Cliente obtiene la posibilidad de continuar el soporte del proyecto por cuenta propia o con la participación de otros especialistas.

Después de la finalización de los trabajos, se recomienda al Cliente:

revocar accesos temporales;

eliminar cuentas temporales;

cambiar contraseñas temporales;

regenerar tokens y claves API;

revisar la lista de usuarios activos y claves de acceso;

asegurarse de que el Prestador ya no tenga acceso técnico a los sistemas del Cliente.

---

13. Principio general de seguridad

La seguridad del proyecto no se basa únicamente en la confianza personal, sino en un proceso controlado.

Incluso si el Cliente no entrega al Prestador bases de datos reales, accesos de producción ni secretos comerciales completos, los trabajos pueden realizarse mediante entornos aislados, datos anonimizados, permisos limitados y código fuente verificable.

Este enfoque permite al Cliente mantener el control sobre su infraestructura, su información confidencial y los resultados del desarrollo en todas las etapas de la colaboración.

Prestador:
Nombre / Razón social: _____
RUC: _____
País de prestación de servicios: República del Paraguay

Cliente:
Nombre / Razón social: _____

Fecha: «_» _____ 20

Firma del Prestador: _____

Firma del Cliente: _____