SEGURIDAD

Anexo de seguridad

Versión 1.0 · 2026-11-05

Presentación

Este Anexo de Seguridad (el «**Anexo**») forma parte del Convenio de Confidencialidad y No Divulgación (el «**Convenio**») que celebran el PROVEEDOR y el CONTRATANTE identificados en su Carátula. Es obligatorio para la Implementación y el Mantenimiento, se firma con el contrato de esos servicios y prevalece sobre el Convenio en las materias que regula, conforme al numeral 20.1 del Convenio. Los términos con mayúscula que no se definen aquí tienen el significado que les da el Convenio.

1. Objeto y alcance

1.1 Este Anexo fija las medidas de seguridad, las reglas de acceso a los sistemas del CONTRATANTE, el tratamiento de los Datos Personales y el cierre del servicio durante la Implementación y el Mantenimiento.

1.2 Es un modelo: los datos de cada Parte constan en la Carátula del Convenio y no se modifican en este texto.

2. De quién es qué

2.1 La Infraestructura Dedicada, es decir, la máquina virtual, la cuenta o el acceso por API al proveedor de Modelos de IA y los agentes, es del PROVEEDOR, que la contrata, la paga y la administra a su nombre. El CONTRATANTE la usa como parte del servicio y paga por ello el precio del servicio; no adquiere propiedad ni posesión sobre ella.

2.2 La información es del CONTRATANTE, incluida la que los agentes acumulen a partir de ella en memorias, índices, bitácoras o bases de datos. El CONTRATANTE puede pedir su exportación y llevársela, conforme a la sección 11.

2.3 El PROVEEDOR no utiliza la información del CONTRATANTE para fines propios, no la usa para entrenar ni ajustar Modelos de IA y no la comparte con otros clientes. Lo anterior no impide conservar los indicadores agregados y anónimos que permite el numeral 6.1, inciso c), del Convenio, que no identifican al CONTRATANTE ni permiten reconstruir su información.

---

3. Cómo se conecta el PROVEEDOR

3.1 El PROVEEDOR se conecta sobre la información del CONTRATANTE, en los sistemas del CONTRATANTE, mediante interfaces de programación (API) o conectores MCP y con las Credenciales que el CONTRATANTE otorga. No extrae, no copia y no conserva esa información para fines propios, salvo los indicadores agregados y anónimos del numeral 6.1, inciso c), del Convenio. Es el CONTRATANTE quien extrae la información de sus sistemas y la entrega cuando corresponde.

3.2 Lo que se almacene en la Infraestructura Dedicada se limita a lo necesario para prestar el servicio y se rige por la sección 11.

---

4. Credenciales y accesos

4.1 **Solo lectura por defecto.** Toda Credencial se entrega como llave API o token de mínimo privilegio, generado por el área de sistemas del CONTRATANTE para cada sistema y con permiso de solo lectura.

4.2 **Escritura con autorización.** El CONTRATANTE puede otorgar permiso de escritura en un sistema únicamente mediante autorización expresa y por escrito para ese sistema. Aun con ese permiso, el agente pide la autorización expresa y por escrito del usuario que lo instruye, en la conversación con el agente, antes de cada acción de escritura, y el PROVEEDOR conserva el registro de cada autorización. Sin autorización por sistema y por acción, el agente no escribe.

4.3 **Resguardo.** Las Credenciales se guardan en la bóveda de secretos que el PROVEEDOR designa por escrito, cifradas, con acceso limitado al personal que las necesita y sin copia en correo electrónico, aplicaciones de mensajería ni herramientas personales. Queda prohibido intercambiarlas por esos medios, conforme al numeral 9.2 del Convenio.

4.4 **Lo que el PROVEEDOR no recibe.** Conforme al numeral 9.3 del Convenio, el PROVEEDOR no recibe la firma electrónica avanzada, los sellos digitales ni la contraseña ante la autoridad fiscal del CONTRATANTE, ni usuarios, claves o dispositivos de banca electrónica. Las fuentes

bancarias y fiscales solo se conectan mediante archivos que entregue el CONTRATANTE o mediante la API del banco o de un proveedor que el CONTRATANTE autorice, con llave o token de solo lectura.

4.5 **Revocación y rotación.** El CONTRATANTE puede limitar o revocar cualquier acceso en cualquier momento. El PROVEEDOR suspende el uso de la Credencial dentro de las 24 horas siguientes a la solicitud escrita del CONTRATANTE y sustituye las Credenciales que caduquen, se revoquen o se vean comprometidas.

---

5. Medidas de seguridad de la Infraestructura Dedicada

5.1 Para cada CONTRATANTE, la máquina virtual, la cuenta o el acceso por API al proveedor de Modelos de IA, los agentes, las memorias y las bitácoras están separados lógicamente de los de otros clientes del PROVEEDOR.

5.2 El PROVEEDOR mantiene, al menos: cifrado de la información en tránsito y en reposo conforme a los estándares de la industria; autenticación de múltiples factores para sus administradores; acceso nominal y de mínimo privilegio; registro de los accesos y de los cambios de configuración; actualización de los componentes con parches de seguridad; y cifrado del almacenamiento de objetos en el que se guardan los entregables. El PROVEEDOR no hace respaldos de la información del CONTRATANTE (sección 11).

5.3 El PROVEEDOR responde por la seguridad de la Infraestructura Dedicada que administra. No hace respaldos de la información del CONTRATANTE ni garantiza su recuperación ante la pérdida o falla del almacenamiento: el CONTRATANTE conserva el original en sus sistemas y pide la exportación de lo que le importe conservar. No responde por la seguridad, las fallas ni las interrupciones de los sistemas del CONTRATANTE que no deriven de su dolo o de su culpa grave, conforme al numeral 9.5 del Convenio, y no realiza pruebas de penetración ni de vulnerabilidades sobre ellos.

---

6. Modelos de inteligencia artificial

6.1 El PROVEEDOR trata la información del CONTRATANTE con Modelos de IA solo mediante las cuentas o accesos por API que contrata y administra, de proveedores que, por sus términos o por la configuración que el PROVEEDOR aplica, excluyen el uso del contenido para entrenar sus modelos, conforme al numeral 8.1 del Convenio. El PROVEEDOR mantiene aplicada esa

configuración mientras dure el servicio y, si un proveedor o un servicio de enrutamiento no la admite, no lo usa para tratar la información del CONTRATANTE.

6.2 El acceso a los modelos se contrata con el proveedor, directamente o mediante un servicio de enrutamiento de modelos, y se conecta al arnés del PROVEEDOR por API. Los modelos pueden ser de distintos proveedores y estar ubicados fuera de México; el PROVEEDOR los identifica en el Anexo 2 del Convenio. El uso incluido en la mensualidad tiene el tope que fijan los términos del servicio.

6.3 Ninguna de las Partes utiliza la información de la otra ni la Información Derivada para entrenar o ajustar Modelos de IA, conforme al numeral 8.4 del Convenio.

---

7. Trazabilidad

7.1 Cada acción del agente deja constancia de cuándo ocurrió, en qué sistema, qué usuario la instruyó y qué autorizó. El CONTRATANTE puede pedir copia de esas bitácoras en cualquier momento durante el servicio.

7.2 Las bitácoras son Información Derivada del CONTRATANTE y siguen la suerte de la sección 11.

---

8. Personal y proveedores

8.1 Solo accede a la información del CONTRATANTE el personal del PROVEEDOR que lo necesita para el Propósito y que está obligado a guardar confidencialidad en términos no menos estrictos que los del Convenio.

8.2 Los proveedores tecnológicos del PROVEEDOR se identifican en el Anexo 2 del Convenio y se sujetan al numeral 8.5 del Convenio. Los proveedores de infraestructura en la nube y de resguardo de secretos de cada CONTRATANTE, y su país, los asienta el PROVEEDOR por escrito en la tabla del numeral 8.3 antes de iniciar la Implementación, y esa tabla complementa el Anexo 2. El PROVEEDOR responde frente al CONTRATANTE por sus actos como si fueran propios, dentro de lo previsto en las Cláusulas Décima Séptima y Décima Octava del Convenio.

8.3 **Proveedores de infraestructura y de resguardo de secretos.** El PROVEEDOR completa esta tabla antes de iniciar la Implementación.

Infraestructura en la nube (máquina virtual y base de datos)

PROVEEDOR

_____

PAÍS DEL TRATAMIENTO

_____

Almacenamiento de objetos para los entregables

PROVEEDOR

_____

PAÍS DEL TRATAMIENTO

_____

Resguardo de secretos (bóveda)

PROVEEDOR

_____

PAÍS DEL TRATAMIENTO

_____

9. Incidentes de seguridad

9.1 El PROVEEDOR notifica por escrito al CONTRATANTE, sin demora injustificada y a más tardar dentro de las 72 horas siguientes a que tenga conocimiento de ello, cualquier vulneración de seguridad o uso no autorizado que afecte la información, las Credenciales o los Datos Personales del CONTRATANTE (numerales 5.1 h) y 10.2 del Convenio).

9.2 El aviso describe qué ocurrió, qué información se afectó, las medidas de contención adoptadas y un contacto. El PROVEEDOR contiene el incidente, revoca o rota las Credenciales afectadas, colabora con el CONTRATANTE y le entrega un informe de causa y remediación dentro de los 10 Días Hábiles siguientes.

9.3 Si el incidente afecta Datos Personales, el CONTRATANTE, como responsable, decide si debe informar a los titulares y a la autoridad conforme al artículo 19 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (la «**LFPDPPP**»); el PROVEEDOR le proporciona la información disponible para ello.

10. Datos Personales

10.1 Respecto de los Datos Personales que el CONTRATANTE pone a disposición del PROVEEDOR, el CONTRATANTE es el responsable y el PROVEEDOR la persona encargada, en términos de la LFPDPPP y de la Cláusula Décima del Convenio. El PROVEEDOR los trata solo conforme a las instrucciones del CONTRATANTE y para el Propósito, adopta las medidas de seguridad administrativas, técnicas y físicas que exige el artículo 18 de la LFPDPPP y no los comunica a terceros, salvo a los proveedores del Anexo 2 que actúan como subencargados y que el servicio requiere, con obligaciones equivalentes a las de este Anexo. Las categorías de datos son las que el CONTRATANTE conecta a los agentes; el tratamiento dura mientras dure el servicio y el plazo de exportación de la sección 11. El PROVEEDOR asiste al CONTRATANTE, dentro de los 5 (cinco) Días Hábiles siguientes a su solicitud, para atender los derechos de acceso, rectificación, cancelación y oposición de los titulares.

11. Terminación, entrega de la información y destrucción

11.1 **Cierre de accesos.** Al terminar el Mantenimiento, el PROVEEDOR revoca de inmediato las Credenciales, cierra los accesos del agente a los sistemas del CONTRATANTE y suspende el uso de la Infraestructura Dedicada.

11.2 **Entregables.** Los reportes, documentos, PDF y hojas de cálculo que genera el agente se envían al correo electrónico del CONTRATANTE o quedan en la conversación del agente en el canal de mensajería, y además se guardan en un almacenamiento de objetos en la nube mientras la suscripción esté activa. El PROVEEDOR no hace respaldos de la información del CONTRATANTE: lo que éste quiera conservar, debe pedir que se le exporte.

11.3 **Exportación.** Durante el servicio y dentro de los 30 (treinta) días naturales siguientes a la Fecha de Terminación, el CONTRATANTE puede pedir por escrito la exportación de la información que quiera, incluidos los entregables guardados y el contenido que los agentes acumularon a partir de ella, y el PROVEEDOR se la entrega en formato estándar y exportable dentro de los 10 (diez) Días Hábiles siguientes a la solicitud. Esa información es del CONTRATANTE.

11.4 **Destrucción.** El PROVEEDOR avisa por correo electrónico al CONTRATANTE 5 (cinco) Días Hábiles antes de iniciarla. Vencido ese plazo, o antes si el CONTRATANTE confirma por escrito que no necesita más exportaciones, el PROVEEDOR destruye de manera segura e irreversible todas las copias de la información del CONTRATANTE, de los entregables y de la Información

Derivada, incluidas las memorias, los índices, las bitácoras, las conversaciones y las representaciones vectoriales, dentro de los 30 (treinta) días naturales siguientes. Las copias que mantengan los proveedores de infraestructura por su propia operación se destruyen conforme al ciclo de esos proveedores (numeral 13.3 del Convenio).

11.5 **Acta.** El PROVEEDOR acredita la entrega y la destrucción con un acta firmada por su representante legal, bajo protesta de decir verdad (numeral 13.2 del Convenio).

11.6 El PROVEEDOR no conserva información del CONTRATANTE después de ese plazo, salvo la que la ley lo obligue a conservar y lo previsto en el numeral 13.3 del Convenio, que sigue sujeto a confidencialidad mientras se conserve.

---

12. Verificación

12.1 Una vez al año, y cuando ocurra un incidente, el CONTRATANTE puede pedir por escrito, con 10 Días Hábiles de anticipación, información razonable sobre el cumplimiento de este Anexo: un cuestionario de seguridad, las evidencias de las medidas de la sección 5 y las bitácoras de la sección 7. La verificación no incluye pruebas de penetración ni acceso a la infraestructura de otros clientes.

---

13. Responsabilidad

13.1 La responsabilidad derivada de la confidencialidad, las Credenciales y los Datos Personales se rige exclusivamente por las Cláusulas Décima Séptima y Décima Octava del Convenio. Este Anexo no establece un régimen de responsabilidad propio.

---

14. Vigencia

14.1 Este Anexo rige desde el inicio de la Implementación y hasta que el PROVEEDOR cumpla la sección 11. Las obligaciones de confidencialidad subsisten conforme a la Cláusula Décima Cuarta del Convenio.

Leído que fue el presente Anexo, las Partes lo firman junto con el contrato de Implementación y Mantenimiento.

EL PROVEEDOR

- Nombre o razón social: _____
- Nombre de quien firma: _____
- Cargo: _____
- Firma: _____
- Fecha: _____

EL CONTRATANTE

- Nombre o razón social: _____
- Nombre de quien firma: _____
- Cargo: _____
- Firma: _____
- Fecha: _____