

Guías Internacionales de Riesgo de Proveedores

Respuestas de riesgo de proveedores país por país más allá de las guías existentes del Golfo, África y UE/Reino Unido — Canadá, Australia, India, Singapur, Japón, Brasil, Suiza, Nueva Zelanda, Corea del Sur y Turquía. Indica claramente qué posee Cyber Crucible y cómo la arquitectura respalda cada régimen.

- [¿Cyber Crucible cumple con la PIPEDA de Canadá y la Ley 25 de Quebec?](#)
- [¿Cyber Crucible cumple con la Ley de Privacidad de Australia y los APP?](#)
- [¿Cumple Cyber Crucible con la Ley de Protección de Datos Personales Digitales de la India \(DPDP\)?](#)
- [¿Cumple Cyber Crucible con la PDPA de Singapur?](#)
- [¿Cyber Crucible cumple con la APPI de Japón?](#)
- [¿Cyber Crucible cumple con la LGPD de Brasil?](#)
- [¿Cumple Cyber Crucible con la Ley Federal de Protección de Datos \(FADP\) revisada de Suiza?](#)
- [¿Cumple Cyber Crucible con la Ley de Privacidad de Nueva Zelanda de 2020 \(Privacy Act 2020\)?](#)
- [¿Cyber Crucible es compatible con la PIPA de Corea del Sur?](#)
- [¿Cumple Cyber Crucible con la KVKK de Turquía?](#)

¿Cyber Crucible cumple con la PIPEDA de Canadá y la Ley 25 de Quebec?

Respuesta breve: Cyber Crucible apoya las obligaciones de una organización canadiense en virtud de la PIPEDA y la Ley 25 de Quebec principalmente mediante el procesamiento en el endpoint y la no recopilación de contenido de clientes, credenciales o claves; por lo tanto, hay muy poca información personal bajo su custodia que deba proteger, divulgar o transferir. Actúa como proveedor de servicios bajo el control de la organización, y cuenta con un acuerdo de procesamiento de datos disponible.

Cómo se alinea

- **Responsabilidad y salvaguardas.** El cifrado sólido, el control de acceso y el procesamiento local respaldan el principio de salvaguardas de seguridad de la PIPEDA.
- **Aspectos específicos de la Ley 25.** Las reformas escalonadas de Quebec agregaron la notificación de infracciones, la privacidad por defecto y normas sobre transferencias fuera de Quebec; el diseño sin recopilación de datos y con capacidad de operar en las instalaciones respalda las preferencias de residencia de datos y limita la exposición en las transferencias.
- **Apoyo ante infracciones.** La información pronta sobre incidentes ayuda a la organización a cumplir con los deberes de notificación de la PIPEDA y la Ley 25.

El límite honesto

El cumplimiento es responsabilidad de la organización; Cyber Crucible es un control de apoyo y un procesador. No posee ninguna certificación canadiense. Un acuerdo de procesamiento de datos y la documentación correspondiente están disponibles en **dpo@cybercrucible.com**.

¿Cyber Crucible cumple con la Ley de Privacidad de Australia y los APP?

Respuesta breve: Cyber Crucible respalda las obligaciones de una entidad australiana en virtud de la Privacy Act 1988 y los Australian Privacy Principles al minimizar los datos —no recopila contenido, credenciales ni claves de los clientes— y al procesar la información localmente en el endpoint. Esto respalda directamente el APP 11 (seguridad de la información personal) y limita la exposición en materia de divulgación transfronteriza bajo el APP 8.

Cómo se alinea

- **Seguridad APP 11** — cifrado, control de acceso y protección autónoma del endpoint.
- **APP 8 transfronterizo** — la implementación local mantiene la información personal en Australia cuando se requiere; no se transfiere contenido del cliente al extranjero para el procesamiento de seguridad.
- **Soporte ante brechas** — información de incidentes para respaldar las obligaciones del esquema de Notifiable Data Breaches.

Notas para la selección de proveedores

El régimen de sanciones de Australia para brechas de privacidad graves o reiteradas se incrementó sustancialmente, lo que agudizó el escrutinio hacia los proveedores. La huella mínima de datos mantiene bajo riesgo al proveedor. La documentación está disponible a pedido.

¿Cumple Cyber Crucible con la Ley de Protección de Datos Personales Digitales de la India (DPDP)?

Respuesta breve: Cyber Crucible respalda las obligaciones de un fiduciario de datos conforme a la Ley de Protección de Datos Personales Digitales de la India al actuar como un procesador de datos que esencialmente no recopila datos personales y procesa en el endpoint. Dado que el contenido del cliente nunca se recopila, las obligaciones de consentimiento, limitación de la finalidad y eliminación tienen una superficie mínima bajo su custodia.

Cómo se alinea

- **Función de procesador** bajo contrato con el fiduciario de datos.
- **Minimización de datos** — no se recopila contenido del cliente, credenciales ni claves.
- **Salvaguardas de seguridad y soporte ante brechas** para las obligaciones del fiduciario.

Notas para la selección de proveedores

India notificó las Reglas DPDP de 2025 en noviembre de 2025, con obligaciones sustantivas que se implementarán progresivamente durante aproximadamente los siguientes 18 meses, por lo que el detalle operativo (gestión del consentimiento, notificación de brechas, mecánicas transfronterizas) aún está entrando en vigor. Mientras tanto, la implementación local (on-premises) respalda las preferencias de residencia de datos. Cyber Crucible no posee ninguna certificación india y respalda, en lugar de asumir, las obligaciones del fiduciario. La documentación está disponible a solicitud.

¿Cumple Cyber Crucible con la PDPA de Singapur?

Respuesta breve: Cyber Crucible respalda las obligaciones de una organización en virtud de la Ley de Protección de Datos Personales de Singapur (PDPA) como un intermediario de datos que procesa en el endpoint y no recopila contenido, credenciales ni claves del cliente. Las obligaciones de Protección y de Limitación de Transferencia tienen poco a lo que aplicarse, ya que hay una cantidad mínima de datos personales bajo su custodia.

Cómo se alinea

- **Rol de intermediario de datos** en virtud de un contrato escrito.
- **Obligación de protección** — cifrado, control de acceso y prevención en el endpoint.
- **Limitación de transferencia** — implementación local (on-premises) y sin transferencia extraterritorial del contenido del cliente para el procesamiento de seguridad.

Notas para la selección de proveedores

La PDPA de Singapur incluye un régimen obligatorio de notificación de brechas de datos; la información oportuna sobre incidentes respalda este requisito. Hay un acuerdo de procesamiento de datos disponible a pedido.

¿Cyber Crucible cumple con la APPI de Japón?

Respuesta breve: Cyber Crucible respalda las obligaciones de un operador comercial en virtud de la Ley de Protección de Información Personal de Japón (APPI, por sus siglas en inglés) al minimizar los datos y procesarlos localmente. No recopila contenido de clientes, credenciales ni claves, por lo que las reglas de manejo, provisión a terceros y transferencia transfronteriza tienen una superficie mínima bajo su custodia.

Cómo se alinea

- **Manejo seguro** — cifrado, control de acceso y protección de endpoints.
- **Transferencia transfronteriza** — la implementación en las instalaciones (on-premises) permite mantener los datos personales en Japón; no se transfiere contenido de clientes al extranjero para el procesamiento de seguridad.
- **Soporte ante brechas** — información de incidentes para respaldar las expectativas de notificación de la APPI.

Notas para la selección de proveedores

Las modificaciones a la APPI reforzaron la notificación de brechas y las reglas transfronterizas; la huella mínima de datos mantiene ligeras las obligaciones del proveedor. La documentación está disponible a solicitud.

¿Cyber Crucible cumple con la LGPD de Brasil?

Respuesta breve: Cyber Crucible respalda las obligaciones de un controlador conforme a la Lei Geral de Proteção de Dados (LGPD) de Brasil, actuando como operador (encargado del tratamiento) que procesa en el endpoint y no recopila contenido, credenciales ni claves del cliente. La mayoría de las obligaciones de la LGPD —base legal, derechos de los titulares de datos, normas de transferencia— tienen una superficie mínima porque hay poca información personal bajo su custodia.

Cómo se alinea

- **Rol de operador** bajo contrato, procesando según las instrucciones del controlador.
- **Medidas de seguridad** — cifrado, control de acceso y prevención autónoma en el endpoint.
- **Soporte ante incidentes** para los deberes de notificación del controlador ante la ANPD.

Notas para la selección de proveedores

La ANPD ha estado cada vez más activa en la aplicación de la ley y en la orientación sobre transferencias; la implementación local (on-premises) respalda las preferencias de residencia de datos. Cyber Crucible no posee ninguna certificación brasileña y respalda los deberes del controlador. La documentación está disponible bajo solicitud.

¿Cumple Cyber Crucible con la Ley Federal de Protección de Datos (FADP) revisada de Suiza?

Respuesta breve: Cyber Crucible respalda las obligaciones de una organización suiza en virtud de la Ley Federal de Protección de Datos revisada (revFADP) al minimizar los datos y el procesamiento localmente en el endpoint. Dado que no recopila contenido de clientes, credenciales ni claves, las obligaciones de seguridad, registros de tratamiento y transferencia tienen una superficie mínima bajo su custodia.

Cómo se alinea

- **Rol de encargado del tratamiento (processor)** bajo un acuerdo de tratamiento de datos.
- **Seguridad por diseño** — el cifrado, el control de acceso y la prevención en el endpoint respaldan el deber de seguridad de datos de la revFADP.
- **Transferencia transfronteriza** — la implementación en las instalaciones mantiene los datos personales en Suiza cuando así se requiere; existen Cláusulas Contractuales Estándar (SCC) disponibles para las transferencias.

Notas para la selección de proveedores

La revFADP se alinea estrechamente con el GDPR, por lo que gran parte del soporte de Cyber Crucible para el GDPR es aplicable también aquí. La documentación, incluidas las SCC, está disponible a solicitud.

¿Cumple Cyber Crucible con la Ley de Privacidad de Nueva Zelanda de 2020 (Privacy Act 2020)?

Respuesta breve: Cyber Crucible respalda las obligaciones de un organismo neozelandés en virtud de la Privacy Act 2020 al no recopilar contenido, credenciales ni claves del cliente, y al procesar la información en el endpoint. Los Principios de Privacidad de la Información (Information Privacy Principles) —en particular el almacenamiento y la seguridad (IPP 5) y la divulgación transfronteriza (IPP 12)— tienen una superficie de exposición mínima, ya que hay poca información personal bajo su custodia.

Cómo se alinea

- **Seguridad IPP 5** — cifrado, control de acceso y protección autónoma del endpoint.
- **IPP 12 transfronterizo** — la implementación en las instalaciones mantiene la información personal dentro de Nueva Zelanda; no se transfiere contenido del cliente al extranjero para el procesamiento de seguridad.
- **Soporte ante infracciones** para las obligaciones del organismo relativas a las infracciones de privacidad notificables.

Notas para la selección de proveedores

La Privacy Act 2020 introdujo la notificación obligatoria de infracciones y los avisos de cumplimiento; la información oportuna sobre incidentes respalda ambos aspectos. La documentación está disponible a solicitud.

¿Cyber Crucible es compatible con la PIPA de Corea del Sur?

Respuesta breve: Cyber Crucible respalda las obligaciones de una organización en virtud de la Ley de Protección de Información Personal de Corea del Sur (PIPA) —uno de los regímenes más estrictos a nivel mundial— al minimizar los datos y el procesamiento en el endpoint. No recopila contenido de clientes, credenciales ni claves, por lo que las obligaciones de consentimiento, manejo y transferencia transfronteriza tienen una superficie mínima bajo su custodia.

Cómo se alinea

- **Rol de encargado del tratamiento (processor)** bajo contrato, según las instrucciones del responsable del tratamiento (controller).
- **Salvaguardas sólidas** — el cifrado, el control de acceso y la prevención en el endpoint respaldan las exigentes expectativas de seguridad de la PIPA.
- **Transferencia transfronteriza** — la implementación local (on-premises) ayuda a mantener la información personal dentro de Corea; no se transfiere contenido de clientes al extranjero para el procesamiento de seguridad.

Notas para la selección de proveedores

La PIPA conlleva sanciones significativas y requisitos de seguridad detallados; la huella mínima de datos y la opción local (on-premises) mantienen el riesgo del lado del proveedor en un nivel bajo. La documentación está disponible a solicitud.

¿Cumple Cyber Crucible con la KVKK de Turquía?

Respuesta breve: Cyber Crucible respalda las obligaciones de un responsable del tratamiento de datos conforme a la Ley de Protección de Datos Personales de Turquía (KVKK) al no recopilar contenido de clientes, credenciales ni claves, y al procesar en el endpoint. Las obligaciones de registro, seguridad y transferencia tienen una superficie mínima porque hay pocos datos personales bajo su custodia.

Cómo se alinea

- **Rol de encargado del tratamiento de datos** bajo contrato.
- **Medidas de seguridad** — el cifrado, el control de acceso y la prevención en el endpoint respaldan el requisito de medidas técnicas de la KVKK.
- **Transferencia transfronteriza** — la implementación local (on-premises) respalda las preferencias de residencia de datos bajo las normas de transferencia de Turquía.

Notas para la selección de proveedores

El régimen de transferencia de la KVKK y las obligaciones de registro en VERBIS recaen en el responsable del tratamiento; Cyber Crucible respalda, y no asume, esas obligaciones. La documentación está disponible a solicitud.