

Cláusulas de ciberseguridad



GRUPO POPULAR



Adquisición de Servicios y Aplicaciones a ser Instalados OnPremises

1. **Virus, otros programas maliciosos y medidas para seguridad de la información.** **EL PROVEEDOR** declara que los sistemas, licencias o suscripciones de soluciones objeto de este acuerdo, estarán habilitados para proteger la Información confidencial y la Información de identificación personal y/o transaccional, de conformidad con la ley y/o normas comerciales aplicables. **EL PROVEEDOR** declara que su desempeño de los Servicios y los Servicios mismos no introducirán virus u otros elementos dañinos diseñados para interrumpir la operación ordenada o dañar la integridad de los archivos de datos residentes en cualquiera de los equipos de **GRUPO POPULAR Y/O SUS FILIALES**. **EL PROVEEDOR** hará todos los esfuerzos posibles para garantizar que, a partir de la fecha en que se entregue cada Entregable a **GRUPO POPULAR Y/O SUS FILIALES**, dicho Entregable no contenga ningún virus u otro elemento dañino. En consecuencia, **EL PROVEEDOR** deberá, con respecto a los sistemas, licencias o suscripciones objeto de este acuerdo, tomar las siguientes medidas de seguridad:
 - a. Eliminar cualquier código informático diseñado para dañar, interrumpir, inhabilitar o impedir de cualquier modo, el funcionamiento ordenado de cualquier software, archivo de datos, firmware, hardware, sistema informático o red ("Virus");
 - b. Garantizar con esfuerzos razonables, durante la redacción, ejecución y copia de cualquier Software entregado en conexión con el Acuerdo, que dicho Software está libre de cualquier Virus, antes de la entrega, de cualquier Software y cualquier medio en el que se deba entregar con una versión actual de una aplicación antimalware líder.
 - c. El Software no contendrá ningún código de computadora ni ningún otro procedimiento, rutina o mecanismo diseñado para: (a) interrumpir, inhabilitar, o dañar de ninguna manera el funcionamiento ordenado del Software basado en el transcurso de un período de tiempo, que exceda un número autorizado de copias, o avance a una fecha particular o cualquier otra medida (algunas veces referidas como "bombas de tiempo", "bloques de tiempo" o dispositivos "mecanismos de desactivación"); (b) causar que el Software dañe o corrompa cualquiera de los datos, medios de almacenamiento, programas, equipos o comunicaciones de cualquiera de los Afiliados del Banco, o la data de sus respectivos clientes, o que interfiera con las operaciones del Banco o sus Afiliados, o (c) permitir a **EL SUPLIDOR**, su Personal, sus licenciantes o cualquier otro tercero, rastrear o monitorear el uso del Software o de los Sistemas del Banco o acceder a estos de otra forma, por cualquier razón (a veces denominado "trampas") códigos de acceso "o dispositivos" puerta trampa ").
 - d. **EL PROVEEDOR** deberá asegurarse que el software adquirido sea desarrollado bajo las mejores prácticas de metodologías de desarrollo seguro.



- e. Realizar pentesting y revisión de código estática y dinámica siempre que se realice algún update del sistema antes de ser entregado a Grupo Popular, para garantizar las buenas prácticas de desarrollo seguro.
2. **Mitigación de Daños.** En adición a, y no en lugar de, las obligaciones de indemnidad de **EL PROVEEDOR**, si algún Servicio o Entregable llega a ser, o es probable que se convierta, en el objeto de un reclamo de un tercero, entonces **EL PROVEEDOR** deberá: (i) adquirir el derecho de **GRUPO POPULAR Y/O SUS FILIALES** y los Indemnizados para continuar utilizando los Servicios o Entregables según lo contemplado en lo adelante; (ii) modificar los Servicios o Entregables y convertirlos en no infractores (siempre que tal modificación no degrade materialmente el rendimiento, el funcionamiento o la operación de los Servicios o Entregables); o (iii) reemplazar los Servicios o Entregables por Servicios o Entregables igualmente adecuados, funcionalmente equivalentes, compatibles y no infractores. Si, a pesar de los esfuerzos de **EL PROVEEDOR** de conformidad con lo anterior, **GRUPO POPULAR Y/O SUS FILIALES** no puede continuar utilizando los Servicios o Entregables, entonces **GRUPO POPULAR Y/O SUS FILIALES** tendrá derecho a rescindir la Orden de trabajo aplicable (en todo o en parte) sobre aviso por escrito a **EL PROVEEDOR**.
3. **Notificación de Reclamos de Terceros.** **EL PROVEEDOR** notificará inmediatamente a **GRUPO POPULAR Y/O SUS FILIALES** sobre cualquier amenaza, advertencia, reclamo o acción contra **EL PROVEEDOR** o sus clientes o proveedores, que podría tener un impacto adverso en el uso de **GRUPO POPULAR Y/O SUS FILIALES** de los Servicios o Entregables proporcionados o puestos a disposición de **GRUPO POPULAR Y/O SUS FILIALES** de conformidad con este Acuerdo.
4. **Cumplimiento.** **EL PROVEEDOR** garantiza que los sistemas, licencias o suscripciones de soluciones que se están contratando y que manejan Información de Identificación Personal y Transaccional, la procesarán de conformidad con este acuerdo, incluyendo, pero no limitándose a la privacidad o protección de datos, a todas las prohibiciones de uso indebido y prácticas desleales y engañosas, y las políticas, normas y leyes aplicables, como los datos de la Industria de Tarjetas de Pago (PCI DSS) y Estándares de seguridad.
5. **Obsolescencia.** **EL PROVEEDOR** garantiza que los sistemas, licencias o suscripciones de soluciones objeto de este acuerdo se encuentran debidamente actualizados a las últimas versiones soportadas disponibles en el mercado. **EL PROVEEDOR** deberá asegurar a **GRUPO POPULAR Y/O SUS FILIALES**, que el producto o solución estará soportado por nuevas actualizaciones y parchado de herramientas que apoyan su ejecución.
6. **Incidentes de seguridad de datos y otros incumplimientos.** **EL PROVEEDOR** notificará a **GRUPO POPULAR Y/O SUS FILIALES** inmediatamente en caso de incumplimiento de sus obligaciones, en caso de que la protección de datos se vea afectada, o cualquier otro Incidente de Seguridad de Datos, pero en ningún caso más de 24 horas después de **EL**



PROVEEDOR, saber o sospechar razonablemente tal evento. A costo de **EL PROVEEDOR**, **EL PROVEEDOR** asistirá y cooperará con **GRUPO POPULAR Y/O SUS FILIALES** con respecto a la comunicación a las partes afectadas, el gobierno o los organismos reguladores, y otras medidas correctivas según lo solicite razonablemente el **GRUPO POPULAR Y/O SUS FILIALES** o según lo requiera cualquier ley o normativa de privacidad o protección de datos aplicable, siempre dicha cooperación incluirá lo siguiente:

- a. **EL PROVEEDOR** investigará rápidamente dicho Incidente de Seguridad de Datos y tomará todas las medidas razonables y necesarias para identificar y mitigar sus efectos, y con el acuerdo previo por escrito de **GRUPO POPULAR Y/O SUS FILIALES**, para llevar a cabo cualquier recuperación u otra acción necesaria para remediar la Seguridad de los Datos, siempre que el incidente afecte el servicio contratado;
- b. **EL PROVEEDOR** deberá proporcionar de manera expedita a **GRUPO POPULAR Y/O SUS FILIALES** toda la información disponible e informes, ya sea borrador o finalizados, con respecto al incidente y deberá preparar un resumen basado en el conocimiento completo de **EL PROVEEDOR** sobre el impacto potencial del Incidente de Seguridad de Datos y la respuesta acciones tomadas o planificadas por **EL PROVEEDOR**;
- c. Tan pronto como sea razonablemente posible, **EL PROVEEDOR** deberá cooperar con **GRUPO POPULAR Y/O SUS FILIALES** para identificar a las personas físicas potencialmente afectadas, y cualquier otra información de contacto conocida;
- d. A pedido del **GRUPO POPULAR Y/O SUS FILIALES** y a expensas de **EL PROVEEDOR**, **EL PROVEEDOR** deberá notificar y remediar adecuadamente a las personas cuya Información de Identificación Personal tenga o pueda razonablemente haber sido afectada por el Incidente de Seguridad de Datos, siempre que sea comprobable la negligencia o incumplimiento del acuerdo por parte de **EL PROVEEDOR** con respecto a sus obligaciones;
- e. **GRUPO POPULAR Y/O SUS FILIALES** **EL PROVEEDOR** no puede divulgar la existencia del Incidente de Seguridad de Datos ni ninguna información relacionada sin la aprobación previa por escrito de **GRUPO POPULAR Y/O SUS FILIALES**, excepto cuando sea necesario para informar al **GRUPO POPULAR Y/O SUS FILIALES**, aseguradores, asesores legales externos y firmas de relaciones públicas, a menos que sea requerido hacerlo de conformidad con la ley o normativa aplicable, en cuyo caso deberá proporcionar al **GRUPO POPULAR Y/O SUS FILIALES** un aviso previo razonable donde lo permita la ley para hacerlo.

7. **GRUPO POPULAR Y/O SUS FILIALES** se reserva el derecho de realizar revisiones periódicas relacionadas al cumplimiento de los controles acordados en el presente contrato. De identificarse algún hallazgo en cualquiera de las infraestructuras de **EL PROVEEDOR**, le será reportado y **EL PROVEEDOR** deberá comprometerse a corregirlo de acuerdo a las mejores prácticas de la industria.