

# Cláusulas de ciberseguridad



**GRUPO POPULAR**



## Plataform As A Service

1. **Seguridad de la infraestructura.** Para asegurar la integridad, confidencialidad y disponibilidad de toda la información y datos de la Grupo Popular y sus filiales, y mitigar la amenaza, riesgo e impacto del uso indebido y abuso externo o interno de la misma, **EL PROVEEDOR** deberá aplicar los siguientes requisitos de seguridad de la información:
  - a. Instalar cortafuegos (firewall) para redes basados en las mejores prácticas de la industria entre los servidores y las puertas de enlace (gateways) a la red pública de modo que excluyan los protocolos de comunicación que no sean necesarios para procesar el tráfico de Internet;
  - b. Proteger el acceso a todos los equipos, de cualquier naturaleza, incluyendo equipos de comunicaciones, servidores, equipos perimetrales, como mínimo, mediante una combinación de la identificación (ID) del usuario y la contraseña secreta, sin que esto implique una limitante para implementar medidas de seguridad de acceso y autenticación adicionales;
  - c. Cambiar las contraseñas mínimo cada noventa (90) días o con más frecuencia;
  - d. Asegurar que sus equipos se encuentren ubicados en zonas físicamente seguras y tengan site alternos en casos de desastres naturales, casos de fuerza mayor o inducidos;
  - e. Reforzar la seguridad de todos los equipos que son utilizados para procesar, almacenar o transmitir datos e información de **GRUPO POPULAR Y/O SUS FILIALES**, en virtud de la ejecución de este contrato, debiendo dicho reforzamiento incluir, entre otros, la eliminación de todos los privilegios y servicios salvo aquellos que sean esenciales para la ejecución de las operaciones para las que están instalados dichos servidores;
  - f. Registrar toda la actividad en la infraestructura (Equipos de comunicaciones, Servidores, Equipos perimetrales) o logs de auditoria, de una manera apropiada por un período continuo y en línea según las mejores prácticas de la industria o por un periodo de retención en línea de acuerdo a lo solicitado por Grupo Popular.
  - g. **GRUPO POPULAR Y/O SUS FILIALES** se reserva el derecho a realizar pruebas de penetración a los servicios ofrecidos por **EL PROVEEDOR**

**PÁRRAFO I:** Para garantizar el cumplimiento de los requisitos de seguridad de la información de **GRUPO POPULAR Y/O SUS FILIALES**, de la normativa legal vigente en la materia, y de las mejores prácticas de la industria para el respaldo y la recuperación de información, **EL PROVEEDOR** deberá:

- a. Implementar medidas de respaldo adecuadas, incluido el almacenamiento de los archivos de datos de respaldo en lugares seguros fuera del sitio de procesamiento, para permitir la recuperación eficiente del sistema;
- b. Facilitar la reanudación de las aplicaciones críticas y actividades de negocios de una manera oportuna después de una emergencia o desastre;



- c. Mantener un plan de recuperación de desastres y/o contingencia documentado para cada sistema crítico relacionado con **GRUPO POPULAR Y/O SUS FILIALES** y para las aplicaciones de negocios, y probarlo anualmente;
- d. Revisar de forma periódicamente todos los controles de seguridad definidos anteriormente para asegurarse de que todavía estén vigentes.

**PÁRRAFO II: 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.

**2. 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.

**3. 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 divulgaciones 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;
- 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** proporcionará a **GRUPO POPULAR Y/O SUS FILIALES** una lista de nombres de 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;
- e. **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.