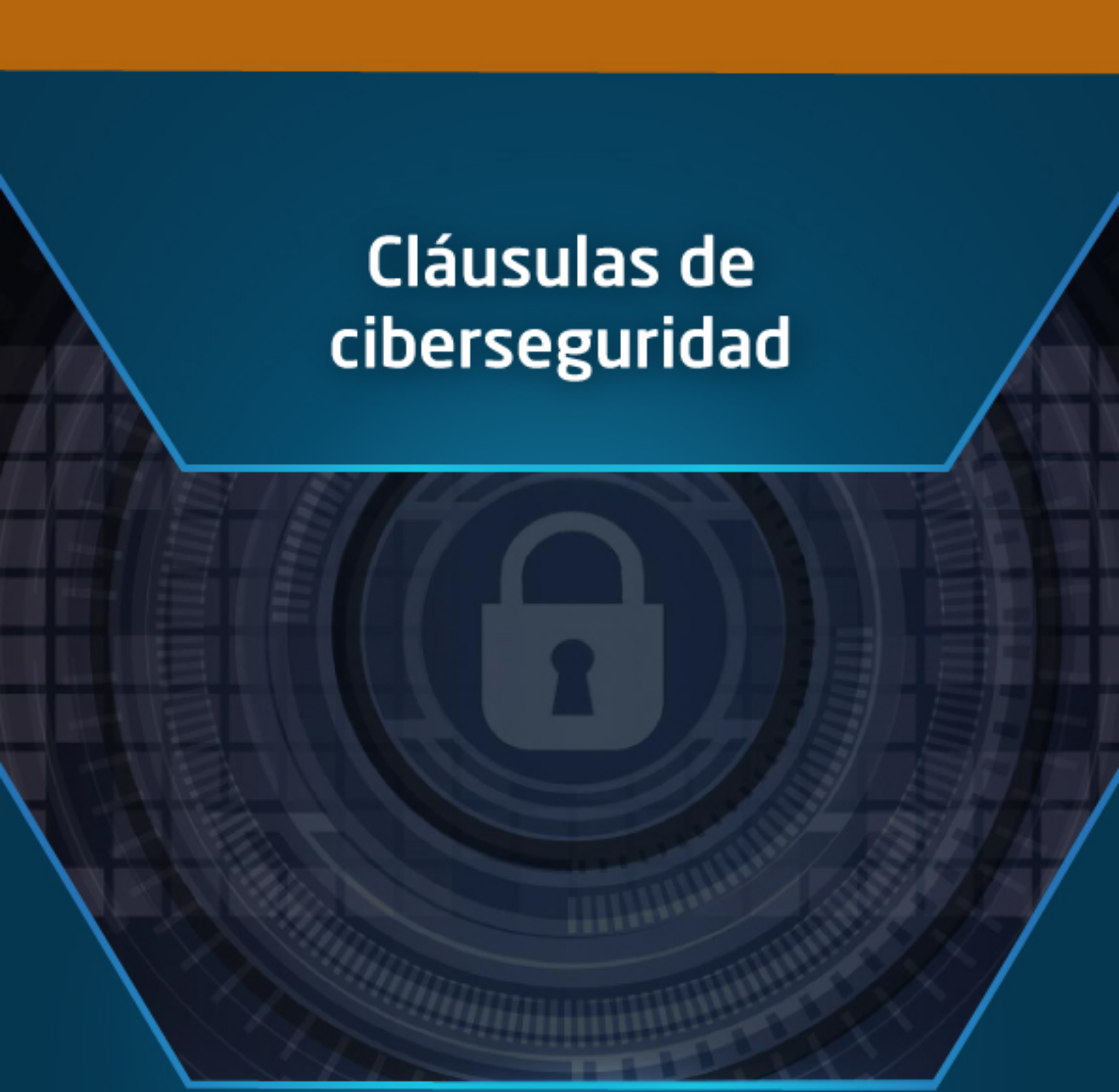
Cláusulas de ciberseguridad



GRUPO POPULAR

Software As A Service

1. **<u>Control de acceso lógico.</u>** **EL PROVEEDOR,** en cumplimiento con los requisitos para el control de la seguridad para el acceso a los sistemas o Softwares, deberá garantizar lo siguiente:
   a. Proteger la confidencialidad de todas las contraseñas o claves de acceso asignadas a **EL PROVEEDOR.**
   b. Contar con una política de contraseñas en virtud de la cual su personal, incluidos los empleados, subcontratistas y/o suplidores de servicios, gestione el cambio de contraseña cada noventa (90) días, evitando contraseñas triviales o evidentes, de conformidad con los mejores estándares de seguridad;
   c. Retirar oportunamente los privilegios de acceso lógico al personal **EL PROVEEDOR.**, incluidos los empleados, subcontratistas y/o suplidores de servicios que, ya sea por transferencia interna o cese de la relación con **EL PROVEEDOR**, o dejen de estar involucrados, por cualesquiera circunstancias, en el procesamiento de la información y datos del **BANCO POPULAR**.

2. **<u>Responsabilidades del personal</u>. EL PROVEEDOR** será directamente responsable por las gestiones que su personal desempeñe en virtud de la ejecución del presente acuerdo y con relación a la información de **BANCO POPULAR**. **EL PROVEEDOR** garantizará que todos los dispositivos utilizados por sus empleados o sus subcontratistas, que estén conectados al ambiente de procesamiento del **BANCO POPULAR**, cumplan y se mantengan cumpliendo los siguientes requisitos de seguridad:

   a. Todo los parchos actualizados de los sistemas operativos y software residentes en los dispositivos, deberán tener el software estándar de la industria contra programas maliciosos (malware) instalado, funcionando y actualizado con el último archivo de firma e instalado y activo con el producto de seguridad tipo cortafuego (firewall) personal y estándar aceptado en la industria.
   b. Todo personal de **EL PROVEEDOR**, ya sea empleados, funcionarios, subcontratistas y suplidores de servicios que vayan a trabajar directamente con información que es perteneciente a **BANCO POPULAR**, deberá mostrar o avalar entrenamientos de seguridad en base a su función (Desarrollo, infraestructura, seguridad, base de datos, etc.) con respecto a las buenas prácticas de seguridad aceptadas en la industria.
   c. **EL PROVEEDOR** deberá asegurarse que el software que sea desarrollado de acuerdo a la prestación del servicio, este bajo las mejores prácticas de metodologías de desarrollo seguro.

3. **<u>Seguridad de la infraestructura.</u>** Para asegurar la integridad, confidencialidad y disponibilidad de toda la información y datos del 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, configurar y activar un sistema integral de protección contra intrusiones (en la red y el host), de conformidad con las mejores prácticas de la industria, para que en forma continua evite, detecte e informe la ocurrencia de ataques no autorizados a la red y en contra de sus sistemas, incluidos, entre otros, intentos de penetración, ataques por denegación de servicio y sondeos excesivos, siendo esta lista enunciativa y no limitativa;
b. 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;
c. Proteger la información de **BANCO POPULAR** contra divulgaciones no autorizada durante su tránsito a través de redes públicas, o su personal autorizado, sus clientes o subcontratistas, garantizando la seguridad de los datos propiedad de **BANCO POPULAR**, utilizando técnicas de criptografías basadas en las mejores prácticas aceptadas en la industria.
d. Proteger el acceso a todos los equipos, de cualquier naturaleza, incluyendo equipos de comunicaciones, servidores, base de datos, y/o equipos perimetrales, como mínimo, mediante una combinación de la identificación (ID) del usuario y contraseña secreta, sin que esto implique una limitante para implementar medidas de seguridad de acceso y autenticación adicionales;
e. Cambiar las contraseñas mínimo cada noventa (90) días o con más frecuencia;
f. 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;
g. Reforzar la seguridad de todos los equipos que son utilizados para procesar, almacenar o transmitir datos e información de **BANCO POPULAR**, en virtud de la ejecución de este contrato, debiendo dicho reforzamiento incluir, entre otros, la eliminación de todos los privilegios de accesos y servicios salvo aquellos que sean esenciales para la ejecución de las operaciones para las que están instalados dichos servidores;
h. Implementar herramientas de análisis de la seguridad o descripción del proceso utilizado para informar periódicamente sobre el estado de cada equipo y verificar que todas las configuraciones, parámetros y opciones estén conformes con el estado de reforzamiento acordado para ese dispositivo y para detectar cambios no autorizados y actualizaciones necesarias a partir de la línea base de la configuración aprobada;
i. Identificar vulnerabilidades y amenazas, e implementar un proceso de investigación continua con fuentes confiables para estas que puedan impactar los ambientes operativos o plataformas utilizados por **EL PROVEEDOR** para el procesamiento de datos del **BANCO POPULAR**,

PÁRRAFO I: Para mitigar la amenaza, riesgo e impacto de los virus informáticos, gusanos, troyanos y otros tipos de software malicioso, colectivamente llamados "malware", **EL PROVEEDOR** deberá:

a) instalar, configurar, activar y mantener actualizado un software anti-malware con capacidad de prevención anti-explotación basado en las mejores prácticas aceptadas en la industria, en todos los equipos que procesen o almacenen las transacciones y cualquier otro dato de **BANCO POPULAR**. Dicho software antimalware deberá estar configurado para invocarlo automáticamente en el arranque y ejecutarlo interactivamente de forma continua, en todos los dispositivos donde esté instalado.

PÁRRAFO II: Para mantener la integridad, confidencialidad y seguridad en general de todas las bases de datos y archivos de datos utilizados para almacenar información y datos del **BANCO POPULAR**, **EL PROVEEDOR** deberá:

a) implementar herramientas de análisis de la seguridad de las bases de datos para revisar periódicamente las configuraciones de dichas bases de datos y garantizar el cumplimiento de las configuraciones de base esperadas, con las mejores prácticas de la industria;
b) Eliminar y destruir de manera adecuada y segura todas las instancias de cualquier información o datos del **BANCO POPULAR** y material impreso para asegurar que las transacciones y demás datos no puedan ser recuperados por personas no autorizadas.
c) Registrar toda la actividad en la infraestructura (Equipos de comunicaciones, Servidores, Base de datos, 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.

PÁRRAFO III: Para garantizar el cumplimiento de los requisitos de seguridad de la información de **BANCO POPULAR**, 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 y para las aplicaciones de negocios relacionadas con **BANCO POPULAR**, el cual debe ser revisado y aprobado anualmente.

PÁRRAFO IV: BANCO POPULAR 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.

4. **Control de cambios en los sistemas.** **EL PROVEEDOR** deberá garantizar el cumplimiento de los requisitos de **BANCO POPULAR,** de la normativa legal vigente en la materia, y de las mejores prácticas aceptadas en la industria, para los controles de cambios, conforme las siguientes pautas, de manera enunciativa y no limitativa, a saber:

    a. Desarrollar, probar y documentar cada cambio de conformidad con la gestión de cambios y las normas, procedimientos y procesos de control, preservando la integridad lógica continua de los datos, programas y rastros de auditorías.
    b. 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.

5. **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.

6. **Incidentes de seguridad de datos y otros incumplimientos**. **EL PROVEEDOR** notificará a **BANCO POPULAR** 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 **BANCO POPULAR** con respecto a divulgaciones a las partes afectadas, el gobierno o los organismos reguladores, y otras medidas correctivas según lo solicite razonablemente el **BANCO POPULAR** 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 **BANCO POPULAR**, 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 **BANCO POPULAR** 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 **BANCO POPULAR** una lista de nombres de las personas físicas potencialmente afectadas, y cualquier otra información de contacto conocida;
d. A pedido del **BANCO POPULAR** 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 **BANCO POPULAR**, excepto cuando sea necesario para informar al **BANCO POPULAR**, 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 **BANCO POPULAR** un aviso previo razonable donde lo permita la ley para hacerlo.