PO-181-0

POLÍTICA DE PRIVACIDAD

MANUAL

MANUAL DE PRIVACIDAD

Aprobaciones	
Dueño de Proceso: Jairo Francisco Gonzalez Matallana	Dr. Yibran Ortegon Botello
Cargo: Gerente de Privacidad, Ciberseguridad y Seguridad de la Información.	**Cargo:** Gerente Integral de Riesgos

TABLA DE CONTENIDO

1 INTRODUCCIÓN POLÍTICAS Y MANUAL DE PROCEDIMIENTOS EN PROTECCIÓN DE DATOS PERSONALES - PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES -PIGDP

La protección de los datos de carácter personal de los ciudadanos ha sido regulada por la legislación colombiana mediante la Ley 1581 de 2012 y el Capítulo 25 del Decreto 1074 de 2015 (Decreto Reglamentario 1377 del 27 de junio de 2013) que reglamenta, desarrolla y complementa la norma general, y establecen las medidas de obligatorio cumplimiento para aquellas entidades que, en el ejercicio de su actividad, sometan a tratamiento este tipo de datos de carácter personal.

El objeto principal de las normas sobre protección de datos personales es salvaguardar el derecho al honor, la intimidad personal y la propia imagen de las personas físicas, atribuyendo determinadas funciones y obligaciones a todas aquellas personas que intervienen en el tratamiento de las bases de datos donde se almacenan los datos de carácter personal.

La Ley consagra igualmente, sanciones para las entidades que incumplan con las obligaciones derivadas de la norma, incluyendo cierre de bases de datos, multas pecuniarias, e inclusive traslado del suceso a las autoridades judiciales, para investigación y/o acusación del delito correspondiente, con las penas privativas de la libertad y pecuniarias a que haya lugar.

El propósito principal de este documento es el de consolidar el conjunto de políticas, principios, medidas, controles, procedimientos y mecanismos que permitan al Banco garantizar el principio de privacidad y la efectiva implementación de la normativa de datos personales y el principio de responsabilidad demostrada.

En este documento se identifican y detallan, los roles, funciones y obligaciones de los empleados y colaboradores del Banco, incluyendo personal contratado a través de empresas temporales o del SENA, o de prestación de servicios, que en su calidad de usuario de las bases de datos del Banco que contengan datos personales de clientes, empleados, proveedores, accionistas y demás personas naturales, tratados por el Banco, le corresponde conocer y respetar.

El Banco a través de este documento declara la importancia por el respeto y la protección de datos personales y considera los datos personales como uno de sus activos más importantes, por lo anterior manifiesta su total compromiso con la implementación, ejecución, seguimiento y mejoramiento continuo del Programa Integral de Gestión de Datos Personales.

Acorde a lo mencionado anteriormente y en concordancia con el decreto 1074 de 2015 se refiere a la responsabilidad demostrada bajo los siguientes términos:

"Los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este decreto, en una manera que sea proporcional a lo siguiente:

1. La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.
2. La naturaleza de los datos personales objeto del tratamiento.
3. El tipo de Tratamiento.
4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares."

El objetivo del Programa Integral de Gestión de Datos Personales es el de permitir contar con altos estándares de protección de datos personales y posibilitar al Banco Popular para que este logre acreditar ante la Superintendencia de Industria y Comercio, el cumplimiento y compromiso en el uso responsable de la información personal suministrada por todos los titulares, así como la adecuada implementación de la ley 1581 de 2012 y demás normativa reglamentaria.

1.1 ESTRUCTURA DEL PIGDP

Ilustración 1

1.2 ÁMBITO DE APLICACIÓN

La presente Política será de aplicación a todo tipo de tratamiento de datos personales que se encuentre bajo la responsabilidad de Banco Popular, incluyendo, pero sin limitar, bases de datos, sistemas de información, aplicativos, soportes físicos, servidores, computadores y/o demás equipos móviles, empleados para el tratamiento de datos personales, que deban ser protegidos de acuerdo con lo dispuesto en la normativa vigente. Aquí se establecen los parámetros, lineamientos y prácticas que debe implementar y vigilar el Banco Popular, para demostrar efectivo cumplimiento a la normativa de datos personales y al principio de responsabilidad demostrada.

1.3 OBJETIVO

Definir el gobierno de datos personales, mediante la definición de lineamientos, responsabilidades, conductas, procedimientos generales, roles, funciones y obligaciones de los responsables y usuarios de la gestión y tratamiento de datos personales, enfocados en proteger la privacidad de los datos personales de clientes empleados, proveedores, accionistas y demás personas naturales, tratados por el Banco.

1.4 ALCANCE

La presente política es de obligatorio cumplimiento para todos los empleados y colaboradores del Banco, incluyendo personal contratado a través de empresas temporales o del SENA, o de prestación de servicios.

La presente Política de Privacidad, define el marco base que guiará la implementación de cualquier directriz, sistema, proceso, procedimiento, y/o acción, relacionados con la Protección de los Datos Personales.

Adicionalmente, la presente Política aplica a todos los datos personales de personas naturales que se hayan recolectado, creado, procesado, almacenado o utilizado en el Banco, sin importar el medio, formato, presentación o lugar en el cual se encuentren.

2 GLOSARIO

AUTORIZACIÓN: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales. Téngase en cuenta que el consentimiento es el eje vertebral de la protección de datos y ello exige que como regla general no se puedan tratar datos de nadie sin su consentimiento, sin perjuicio de que en ocasiones esta obligación esté exenta. Por ejemplo: cuando los datos se traten en el marco de la relación comercial, laboral o administrativa, o cuando por disposición de una norma no sea necesaria la citada autorización.

BASE DE DATOS: Conjunto organizado de datos personales que sea objeto de Tratamiento. Siempre que exista un conjunto de datos personales organizados mediante algún criterio, nos encontraremos ante la existencia de una base de datos. Por ejemplo, una aplicación informática de nóminas constituye una base de datos, pero también lo puede constituir una tabla de datos en formato Word, sin olvidar que también es aplicable este concepto a los datos no automatizados, como una carpeta o archivo en A-Z.

CESIÓN: Revelación de datos realizada a una persona distinta del interesado.

COMUNICACIÓN DE DATOS: Es el resultado de toda revelación de datos personales realizada a una persona distinta del interesado, en desarrollo de una transmisión, trasferencia o cesión de datos personales.

DATO PERSONAL: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Es decir, cualquier dato que podamos relacionar con personas físicas o que permita su identificación.

DOMINIO DE INFORMACIÓN: Los dominios de información son un conjunto de datos lógicamente agrupados por funciones de negocio y son la base para la implementación del modelo de gobierno y gestión de información.

ENCARGADO DEL TRATAMIENTO: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. El encargado del tratamiento es un tercero (normalmente una empresa, pero no necesariamente) que le presta un servicio al responsable del tratamiento y que para ello requiere acceder a datos personales del responsable. Ejemplos de esta definición, son las empresas que contrata el Banco para realizar gestión de cobranzas, call center, mensajería, empresas de mantenimiento de hardware o software, etc. La relación entre el responsable y el encargado se debe regular mediante un contrato de tratamiento de datos personales.

LIDER DE DOMINIO: Líder de negocio y/o reconocido experto en la materia designado como el responsable de todos los aspectos asociados a la gobernabilidad y gestión de la información para su dominio de información, a través de la coordinación de las diferentes partes interesadas relacionados con el dominio asignado representando los intereses en términos de información para las partes interesadas y el Banco.

OFICIAL DE PROTECCIÓN DE DATOS PERSONALES: Es la persona o área designada por el Banco, con el rol principal de velar por la implementación efectiva de las políticas y procedimientos adoptados por el Banco para el cumplimiento de la norma de protección de datos personales, así como la implementación de buenas prácticas de gestión de datos personales dentro de la empresa.

RESPONSABLE DEL TRATAMIENTO: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. Dado el alcance de la presente Política, el responsable del tratamiento de Datos Personales es el Banco Popular S.A.

TITULAR: Persona natural cuyos datos personales sean objeto de Tratamiento.

TRANSFERENCIA: La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

La transferencia ocurre cuando el responsable comparte los datos personales con un tercero, para que éste les dé un **tratamiento por su propia cuenta** y para las finalidades que defina en la autorización otorgada por el Titular.

TRANSMISIÓN: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable.

La transmisión ocurre cuando quien comparte los datos personales, limita el tratamiento de los mismos a una o varias finalidades determinadas por el responsable dentro del contrato y por el titular en su autorización. Este tercero actuará **por cuenta del responsable** y adquirirá la calidad de “encargado” de los datos personales.

TRATAMIENTO: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

USUARIOS: sujeto o proceso autorizado a acceder a datos o recursos. Normalmente un usuario será una persona que accede a datos personales tratados por el Banco. El usuario podrá tener diferentes perfiles de acceso y ser un usuario interno o externo (un usuario de otra organización que accede a nuestro sistema para prestar un servicio, por ejemplo, para soporte técnico).

3 NIVELES DE RIESGO DE LOS DATOS

El riesgo en el tratamiento de los datos se ha clasificado en tres niveles, según la tipología y sensibilidad de los datos contenidos en las bases de datos: nivel básico, medio y alto.

NIVEL	TIPO / DESCRIPCIÓN
Bajo	**Dato público**. Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas. Esta definición, no implica desconocimiento de los principios y obligaciones del Banco en el tratamiento de datos personales públicos. Ejemplos: Nombre, estado civil, número de identificación, fecha de nacimiento, lo relativo a su profesión u oficio.
Medio	**Datos relativos a la Ley 1266 de 2008:** Datos de tipo financiero, crediticio, comercial, de servicios. Ejemplos: Historias crediticias, datos financieros, reporte en las centrales de riesgo. **Dato semiprivado**: dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector o grupo de personas o a la sociedad en general. **Dato privado**: dato que por su naturaleza íntima o reservada solo es relevante para el titular Ejemplos: Correo electrónico, número telefónico de contacto, dirección personal, datos laborales, académicos.
Alto	**Datos sensibles**: aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos. Ejemplos: Datos ideológicos, políticos, religiosos, preferencias sexuales, pertenencia a sindicatos, datos étnicos, salud, huellas dactilares, fotografías, videos y estilos de vida.

Tabla 1

4 INVENTARIO DE BASES DE DATOS

4.1 IDENTIFICACIÓN DE BASES DE DATOS PERSONALES

El Banco dentro del proceso para identificar, inventariar y actualizar sus bases de datos, ha establecido como criterios generales los siguientes:

4.1.1 Finalidades

El Banco ha identificado las bases de datos de acuerdo con su finalidad. Lo anterior bajo el entendido que una base de datos central e inscrita puede segregarse en otras descentralizadas que responden a un mismo contenido y propósito, pero responde a distintas formas de tratamiento o puede encontrarse en repositorios diferentes a la base central.

4.1.2 Forma de Tratamiento

- Base de datos automatizada
  El Banco identifica como base de datos automatizada aquella que se almacena y administra con la ayuda de herramientas informáticas o sistemas de información automatizados.

- Base de datos física (papel)
  El Banco identifica una base de datos física o manual cuando contiene archivos cuya información se encuentra organizada y almacenada de manera física.

El inventario de bases de datos personales que están registradas ante la Superintendencia de Industria y Comercio se presenta según la forma electrónica F.1.10.4.0101 Novedades De Bases De Datos Cambios Sustanciales, teniendo en cuenta su debido diligenciamiento de acuerdo con el A-181-00101 Anexo Diligenciamiento de Formato Novedades de Bases de Datos Cambios Sustanciales.

5 GOBIERNO PARA LA GESTION DE LA PRIVACIDAD

Banco Popular debe estructurar las funciones y responsabilidades frente al Riesgo de Privacidad y frente a la gestión de los riesgos de Privacidad. Este marco de referencia define el esquema de las tres líneas de defensa, considerando la gestión por línea de negocio, una función de gestión de riesgo de Privacidad independiente y una revisión independiente.

Primera Línea (Operación)

- Identificar, evaluar, gestionar y mitigar los riesgos asociados a la privacidad.
- Guiar el desarrollo e implementación de las políticas y procedimientos internos que aseguren que las actividades efectuadas son consistentes con requerido en la ley 1581 de 2012 y sus decretos reglamentarios así como de las políticas y lineamientos internos.
- Implementar acciones correctivas para hacer frente a deficiencias de su proceso y sus controles.

Segunda Línea (Gobierno)

- Establecer los lineamientos, Políticas, estándares, roles y responsabilidades para la gestión de la privacidad.
- Realizar monitoreo y seguimiento continuo a la implementación de prácticas efectivas de gestión de riesgos por parte de la Primera Línea.
- Alertar a la primera línea de asuntos emergentes y de cambios en los escenarios de riesgos.

Tercera Línea (Control)

- Evaluar el cumplimiento de las políticas, lineamientos y procedimientos relacionados con la Privacidad de acuerdo con su plan de trabajo.

6 ROLES Y RESPONSABILIDADES

Para dar cumplimiento a los objetivos de la presente Política de Privacidad, se han definido dentro del Banco las siguientes funciones y obligaciones específicas, y de acuerdo con lo establecido en los Anexos A-181-00102 Generación De Reportes Como Parte Del PIGPD y A-181-00103 Requerimientos Contratación Encargados del Tratamiento De Los Datos Personales cuando estos apliquen:

6.1 6.1 ALTA DIRECCIÓN

La alta dirección del Banco es responsable del aseguramiento de los procesos y procedimientos que sean necesarios para el funcionamiento del Programa Integral de Gestión de Protección de Datos y Responsabilidad Demostrada así mismo que los anteriores, se establezcan, implementen, ejecuten, mantengan y mejoren. El Banco

realizará la gestión necesaria para mantener una efectiva protección de los datos más allá las mínimas obligaciones legales que pueda tener.

6.2 GERENCIA INTEGRAL DE RIESGOS

- Designar la persona o área que asumirá la función de Oficial de Protección de Datos Personales dentro de la organización.
- Aprobar y monitorear el programa integral de gestión de datos personales.
- Informar a la Junta Directiva sobre la ejecución del programa integral de gestión de datos personales.
- Establecer junto con el Oficial de Protección de Datos Personales, las responsabilidades específicas para las otras áreas del Banco respecto a la recolección, almacenamiento, uso, circulación, eliminación o disposición final de los datos que se tratan.

6.3 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

Banco Popular ha decidido designar al Gerente de Privacidad, Ciberseguridad y Seguridad de la Información para asumir la función de Oficial de Protección de Datos Personales.

Las funciones asignadas al Oficial de Protección de Datos Personales, además de todas aquellas que generalmente establecen las leyes de protección de datos personales vigentes, son las siguientes:

- Velar por la implementación efectiva de las políticas y procedimientos adoptados, para dar cumplimiento a las leyes y normativa vigente, así como la implementación de buenas prácticas de gestión de datos personales dentro del Banco.
- Establecer los lineamientos requeridos para garantizar una adecuada administración y protección de la información contenida en las bases de datos.
- Estructurar, diseñar y administrar el programa que permita al banco cumplir las normas sobre protección de datos personales y establecer los controles del programa, su evaluación y revisión permanente.
- Promover la implementación de un sistema que permita administrar los riesgos del tratamiento de datos personales.

- Servir de enlace y coordinador con las demás áreas de la organización para asegurar una implementación transversal del Programa Integral de Gestión de datos Personales.

- Impulsar una cultura de protección de datos dentro de la organización.

- Registrar las bases de datos de la organización en el Registro Nacional de Bases de Datos y actualizar el reporte con relación a la información entregada por parte de las diferentes áreas responsables y líderes de dominio de datos, siempre atendiendo a las instrucciones emitidas por la SIC.

- Revisar los contenidos de los contratos de transmisión nacionales e internacionales de datos que se suscriban con Encargados residentes y no residentes en Colombia.

- Velar por la implementación de planes de monitoreo para verificar el cumplimiento de sus políticas de tratamiento de la información personal.

- Acompañar y asistir al Banco en la atención de las visitas y los requerimientos que realice la Superintendencia de Industria y Comercio

- Realizar seguimiento al Programa Integral de Gestión de Datos Personales

- Revisar y actualizar periódicamente las políticas que deben ser implementadas en Banco Popular para la protección de los datos personales, las cuales deben ser aprobadas por la Gerencia Integral de Riesgo.

- Valorar los incidentes de seguridad de la información relacionados con datos personal con el fin de establecer las medidas correctivas que ameriten y su posterior reporte a la Superintendencia de Industria y Comercio, en caso de considerarlo necesario.

- Monitorear el cumplimiento de las políticas y lineamientos establecidos en esta Política de Privacidad, verificando que estén acordes con lo dispuesto por la regulación vigente.

- Participar en el desarrollo de nuevos procesos, productos o servicios con el fin de verificar el cumplimiento de la normatividad de protección de datos personales vigente.

6.4 FUNCIONES ASIGNADAS A LA GERENCIA DE PRIVACIDAD, CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN

- Definir y mantener políticas sobre la seguridad de la información, que es

almacenada en los medios electrónicos y físicos de la entidad.

- Adoptar las medidas necesarias para que los usuarios de Banco Popular conozcan las políticas de seguridad de la información, así como las consecuencias en que pudieran incurrir en caso de incumplimiento de las mismas.

- Establecer los controles de Seguridad de la Información y Ciberseguridad, tanto a nivel técnico como de seguridad física, que deben tener en cuenta los encargados en los servicios tercerizados cuando se almacenen y/o traten datos personales.

- Monitorear que los lineamientos de seguridad establecidos para la protección de la privacidad de los datos en los sistemas de información sean ejecutados adecuadamente.

- Consolidar un inventario de las bases de datos personales en poder de la organización y calificarlas según su tipo (automatizadas o físicas), a ser reportadas a la Superintendencia de Industria y Comercio.

- Sugerir un programa de entrenamiento en protección de datos personales dirigido a los empleados del Banco.

- Implementar las mejores prácticas con relación a la gestión de seguridad de la información.

6.4 LIDERES DE PROCESOS DEL BANCO

- Incorporar el cumplimiento de las políticas de protección de datos dentro de las actividades de los procesos a su cargo Anexos A-181-00102 Generación De Reportes Como Parte Del PIGPD

- Asegurar que dentro de los flujos de productos a través de los diferentes canales. se solicité de manera previa expresa e informada, la autorización para el tratamiento de datos personales a los titulares de datos, siempre que se vaya a recolectar información personal.

- Asegurar que se cuente con la autorización de tratamiento de datos personales por parte de los titulares, en los casos en los que se realice consulta de datos y previo al cargue de los mismos, cuando estos datos son traídos de fuentes de origen externo.

- Mantener la evidencia (física y/o digital.) de la autorización para el tratamiento de datos personales de los titulares que haya dado su consentimiento a través de los distintos canales

- Asegurar que toda la información de clientes persona natural que requiera ser

gestionada sea extraída de la única fuente oficial que contiene los datos personales de los clientes en el Banco.

- Colaborar con la Gerencia de Privacidad, Ciberseguridad y Seguridad de la Información en la ejecución de las actividades relacionadas con el tratamiento de datos personales dentro de sus áreas de responsabilidad.

- Propender porque en los procesos del Banco, se implementen la totalidad de mecanismos necesarios para la protección de datos personales, emitidos por el organismo de vigilancia y control, así como por la Gerencia de Privacidad, Ciberseguridad y Seguridad de la Información.

- Solicitar el acompañamiento a la Gerencia de Privacidad, Ciberseguridad y Seguridad de la Información, desde el inicio, en los proyectos y/o requerimientos, o ante cambios en procesos o programas en los cuales se traten datos personales, con el propósito de que estos cuenten con los requisitos necesarios para la protección de datos personales antes de su puesta en operación.

- Documentar el proceso de generación de reportes como parte del Programa Integral de Gestión de Datos Personales.

- Verificar que, con anterioridad a la implementación o modificación de los sistemas de información, las pruebas no se realicen con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de base de datos tratada.

- Implementar todas las medidas requeridas por la normativa de protección de datos personales, en los aplicativos y bases de datos a cargo de sus áreas para dar cumplimiento a la normativa de protección de datos.

- Verificar que los traslados de documentación hacia empresas externas de gestión documental, se realice bajo medidas de seguridad y confidencialidad apropiadas.

- Proteger los activos de información del Banco que contengan datos personales a través del cumplimiento de la política de seguridad de la información y ciberseguridad, incluyendo el reporte de incidentes que pongan en riesgo la información personal.

- Definir el valor y la criticidad de la información personal que se custodia, procesa o transporta a través del activo de información; y con base en esta, definir los privilegios de su uso y generar los mecanismos para garantizar las condiciones mínimas de seguridad y mitigación de los riesgos asociados a los mismos.

- Verificar que la información sensible que pueda ser almacenada localmente en equipos sea eliminada de los mismos o conservada en carpetas o servidores una vez ha concluido el uso para la que fue tratada en esos equipos.

- Solicitar acompañamiento a la Gerencia de Privacidad, Ciberseguridad y Seguridad, cuando se celebren contratos u órdenes de servicio en los que se vaya a ejecutar algún tipo de tratamiento sobre datos personales como transmisiones, o transferencias de datos a encargados o responsables del tratamiento.

- Aportar en los tiempos estipulados por la ley 1581 de 2012, la información necesaria a la Gerencia de Operaciones de Servicio al Cliente PQR, cuando se presenten solicitudes de atención de derechos por datos personales, por parte de los titulares de los datos y se requiera dar trámite y respuesta. Así mismo, prestar el acompañamiento pertinente ante requerimientos especiales por parte de la Superintendencia de Industria y Comercio.

- Identificar todos aquellos terceros, proveedores o aliados que actúan como encargados de datos personales, a fin de reportarlos a la Gerencia de Privacidad, Ciberseguridad y Seguridad de la Información.

- Validar que los terceros cuenten con condiciones y medidas de seguridad implementadas que garanticen la Privacidad y confidencialidad de la información automatizada y física con relación a los datos personales entregados por el Banco y que estas sean incluidas dentro de los contratos establecidos.

- Reportar a la Gerencia de Privacidad, Ciberseguridad y Seguridad de la Información, los cambios sustanciales o actualizaciones de las bases de datos o los datos de los encargados a su cargo, con relación a la información que se haya registrado en el Registro Nacional de Bases de Datos.

- Garantizar que previo al inicio de las actividades por parte de los terceros encargados, se haya suscrito el contrato de transmisión o transferencia de datos personales según sea el caso.

- Presentar recomendaciones al Oficial de Protección de Datos Personales, que sirvan para mejorar los procesos relacionados con la materia al interior de la entidad.

6.5 GERENCIA DE GESTIÓN Y DESARROLLO DEL TALENTO HUMANO Y GERENCIA DE ATENCIÓN AL TALENTO HUMANO

- Obtener de los empleados y candidatos las autorizaciones pertinentes para el manejo de su información personal antes y durante la relación laboral.

- Atender oportunamente las consultas y reclamos por datos personales enviadas o realizadas por los empleados vinculados o desvinculados del Banco.

- Establecer planes de formación transversales para todos los empleados y cargos del Banco Popular.

- Realizar el entrenamiento necesario a los nuevos empleados, que tengan acceso por las condiciones de su cargo y funciones, a datos personales gestionados por el Banco.

- Medir la participación, y calificar el desempeño, en los entrenamientos de protección de datos.

- Promover capacitaciones a los funcionarios de la entidad y a terceros en torno a la importancia del cumplimiento de la protección de datos personales.

- Comunicar de forma eficiente al área de Tecnología la desvinculación de los empleados a más tardar el día en que se retira.

- Verificar que en todos los procesos de bienestar donde se capturen o puedan capturar datos de menores de edad, se recolecte de padres y tutores la debida autorización para su tratamiento.

- Establecer los controles oportunos para que únicamente el personal autorizado en el área tenga acceso a la información sensible.

- Verificar que los traslados de documentación de carácter sensible hacia empresas externas de archivo, se realiza bajo medidas de seguridad y confidencialidad apropiadas.

- Verificar que las transmisiones y transferencias de datos personales se realizan bajo los lineamientos de la Gerencia de Privacidad, Ciberseguridad y Seguridad de la Información.

6.6 GERENCIA DE ABASTECIMIENTO ESTRATÉGICO Y DE LA DIRECCIÓN DE INFRAESTRUCTURA

- Atender oportunamente las consultas y reclamos por datos personales enviadas o realizadas por los proveedores, arrendadores y contratistas personas naturales del Banco.

- Obtener de los proveedores personas naturales, arrendadores y de los representantes legales las autorizaciones pertinentes para el manejo de su información personal antes y durante la relación contractual con el Banco.

- Obtener la autorización para el manejo de la información sensible (video grabaciones) de los contratistas que realizan labores en las instalaciones del banco, antes y durante la relación laboral.

- Solicitar a los proveedores la Política de Tratamiento de Datos Personales y el

Manual de Seguridad de la Información, cuando la Gerencia de Privacidad, Ciberseguridad y Seguridad de la Información lo considere necesario.

- Informar a todas las áreas del Banco que soliciten la contratación de un servicio que implique cualquier tipo de tratamiento de datos personales, que deben contar con un concepto emitido por parte de a Gerencia de Privacidad, Ciberseguridad y Seguridad de la Información desde el comienzo de la iniciativa que contenga los lineamientos de protección de datos personales.

- Debe garantizar el cumplimiento de lo consignado en el y A-181-00103 Requerimientos Contratación Encargados del Tratamiento De Los Datos Personales.el cual debe tenerse en cuenta para la contratación de encargados del tratamiento de datos personales

6.7 VICEPRESIDENCIA JURÍDICA

- Brindar asesoría a los líderes de proceso en el entendimiento de la normatividad de protección de datos personales, así como la elaboración y revisión de documentos y clausulados legales.

- Construir y enviar a las áreas que lo requieran, el contrato de Transmisión o Transferencia de Datos Personales, según aplique, bajo los lineamientos establecidos en la normativa vigente sobre protección de datos personales.

- Incluir la cláusula de protección de datos personales en los contratos de servicio cuando el tercero, proveedor o aliado que se esté contratando realice el tratamiento de datos personales.

- Apoyar a la Gerencia de Operaciones de Servicio al Cliente- PQRs en la validación de la respuesta planteada a los Titulares que interponen una consulta o un reclamo en el Banco.

- Monitorear y hacer seguimiento a la legislación y normatividad expedida en materia de protección de datos personales y realizar recomendaciones de ajustes al interior de la entidad.

6.8 GERENCIA DE TECNOLOGÍA Y PRODUCTIVIDAD

- Implementar los aspectos técnicos en los aplicativos y bases de datos para el cumplimiento de la normativa de acuerdo con las solicitudes y requerimientos de los líderes de proceso.

- Entregar de forma oportuna la información requerida por la Gerencia de

Operaciones de Servicio al Cliente PQR, para dar respuesta a las consultas y reclamos de los Titulares o de las autoridades competentes.

6.9 LIDERES DE AREAS COMERCIALES Y DE MERCADEO

- Asegurar que los flujos de índole comercial, o futuras iniciativas en las cuales se requiera recabar y realizar tratamiento de datos personales, se cuente con la autorización para el tratamiento de datos de los titulares.

- Verificar que en todos los procesos de mercadeo potencial se implementan los mecanismos necesarios para recabar previamente las autorizaciones de los potenciales clientes para posteriores tratamientos.

- Verificar que, en todos los procesos de vinculación de clientes, se cuentan con las debidas autorizaciones por parte de los titulares para todas las finalidades previstas.

- Verificar que la fuerza comercial (especialmente la externa), ha sido debidamente formada en materia de protección de datos personales, procedimientos implementados en la organización, responsabilidades y consecuencias de su incumplimiento.

- Verificar que previo a la ejecución de campañas comerciales se cuente con la autorización para el tratamiento de datos del titular y que este último no haya solicitado una exclusión de las interacciones por campañas comerciales a través de SMS, Email o llamadas telefónicas. De ser así deberá ser excluido de estos procesos.

- Verificar que no se generen bases de datos descentralizadas por parte de la fuerza comercial interna o externa que puedan vulnerar el principio de calidad del dato.

6.10 GERENCIA OPERACIONES SERVICIO AL CLIENTE – PQR

- Enviar, solicitar el acompañamiento y hacer seguimiento a las diferentes áreas y líderes de dominio del Banco para su respectiva investigación sobre consultas y reclamos presentados por los titulares, que se pueden derivar del ejercicio de los derechos en materia de Protección de Datos Personales y se deba validar información de productos, canales o cualquier tipo de interacción con el titular o tratamiento realizado con los datos personales almacenados en el Banco con el objetivo de dar trámite a la solicitudes de derechos de los titulares.

- Reportar la información requerida por la Gerencia de Privacidad, Ciberseguridad

y Seguridad de la Información, relacionada con las solicitudes de atención de reclamos relacionados con la protección de datos personales recibidas por el Banco, así como la actualización de aquellos que actúan como encargados de los datos personales y las bases de datos registradas por el Banco ante la SIC.

- Dar respuesta a todas las solicitudes presentadas en los diferentes medios habilitados por Banco Popular que se pueden derivar del ejercicio de los derechos de los titulares en materia de Protección de Datos Personales, dentro de los tiempos establecidos por la ley 1581 de 2012, decretos reglamentarios y demás normatividad vinculante.

- Cuando se requiera, solicitar apoyo a la Dirección de Estudios Jurídicos Institucionales de la Vicepresidencia Jurídica, para la construcción de la respuesta a los requerimientos trasladados por la Superintendencia de Industria y Comercio en materia de Protección de Datos Personales.

- Cuando se requiera apoyo jurídico, solicitar acompañamiento a la Gerencia de Negocios Bancarios de la Vicepresidencia Jurídica, para la construcción de la respuesta a las quejas, peticiones o reclamos de los Titulares en materia de protección de Datos Personales

- Implementar una tipología para la debida categorización en la radicación de las consultas y reclamos por datos personales siguiendo los lineamientos entregados por la Gerencia de Privacidad, Ciberseguridad y Seguridad de la Información del Banco.

- Enviar mensualmente el reporte de la gestión de las solicitudes relacionadas con protección de datos personales a la Gerencia de Privacidad, Ciberseguridad y Seguridad de la Información.

7 OBLIGACIONES GENERALES

El personal que, para el correcto desarrollo de su labor, tiene autorizado el acceso a datos personales, incluyendo al personal de los Encargados, tiene las siguientes obligaciones:

- El personal en general, Lideres de área, Gerentes o Directores que tengan a su cargo la supervisión del cumplimiento de contratos de servicios o alianzas con terceros o proveedores y que realicen cualquier tipo de tratamiento de datos personales de clientes, usuarios o empleados, deberán reportar de forma periódica la información solicitada para la actualización de la información relacionada con los Encargados como tratamientos, finalidades, tipos de datos y

política de protección de datos así como toda la información concerniente a las bases de datos con información personal de acuerdo a lo establecido en el proceso P-181-00101Gestión de Novedades de Bases de Datos Registradas ante la SIC V2.Guardar la confidencialidad respecto a cualquier tipo de información de carácter personal conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con Banco Popular.

- Guardar todos los soportes físicos y/o documentos que contengan información con datos de carácter personal en un lugar seguro, cuando estos no sean usados, particularmente fuera de la jornada laboral.

- Queda prohibido el traslado de cualquier soporte, con datos de carácter personal sensible en los que se almacene información de titularidad del Banco fuera de las instalaciones de esta, sin validación previa de la Gerencia de Privacidad, Ciberseguridad y Seguridad de la Información. En el supuesto de existir traslado o distribución de soportes y documentos sensibles o de riesgo alto, se debe realizar mediante mecanismos que impidan el acceso, uso o manipulación de la información por partes de terceros no autorizados.

- Podrá realizarse creación de bases de datos de carácter temporal o copias de documentos en los que se almacenan datos de carácter personal, generados para el cumplimiento de una necesidad determinada o trabajos puntuales y auxiliares, siempre y cuando su existencia no sea superior a un mes. Estas Bases de Datos de carácter temporal o copias de documentos deberán cumplir con los niveles de seguridad adecuados en función de la tipología o riesgo de los datos y deberán ser borrados o eliminados una vez hayan dejado de ser necesarios para los fines que motivaron su creación.

- Únicamente las personas autorizadas podrán introducir, modificar o anular datos personales desde los aplicativos hacia las Bases de Datos. No está permitido ingresar datos directamente a la Base de Datos, en caso de requerirse se debe seguir lo establecido dentro de los lineamientos del modelo de Seguridad de la Información para adoptar las medidas oportunas sobre el mismo.

- Los permisos de acceso de los usuarios son concedidos por el área encargada de tecnología de acuerdo con perfiles establecidos por cargo.

- Comunicar a la Gerencia de Privacidad, Ciberseguridad y Seguridad de la Información, las incidencias de seguridad de las que tenga conocimiento y que puedan afectar a bases de datos, soportes o documentos que contengan información personal.

7.1 RESPECTO A BASES DE DATOS AUTOMATIZADAS

- Cambiar las contraseñas los usuarios administradores de forma periódica.

- Cerrar o bloquear todas las sesiones al término de la jornada laboral o en el supuesto de ausentarse temporalmente de su puesto de trabajo, a fin de evitar accesos no autorizados.

- No copiar la información contenida en las Bases de Datos en los que se almacenen datos de carácter personal (en especial sensibles) en el computador personal, cd, discos externos, USB o a cualquier otro soporte.

- Los usuarios tienen prohibido el envío de información de carácter personal sensible o de nivel de riesgo alto. En todo caso, este envío únicamente podrá realizarse si se adoptan los mecanismos necesarios para evitar que la información no sea inteligible ni manipulada por terceros.

- Los usuarios no podrán instalar cualquier tipo de programas informáticos o dispositivos ni en los servidores centrales ni en el computador empleado en el puesto de trabajo.

- Queda prohibido:

  - ✓ Emplear usuarios y contraseñas de otros usuarios para acceder al sistema.
  - ✓ Infringir las medidas de seguridad establecidas en los sistemas informáticos, intentando acceder a Bases de Datos o programas cuyo acceso no le haya sido permitido.
  - ✓ Y en general, el empleo de la red corporativa, sistemas informáticos y cualquier medio puesto al alcance del usuario vulnerando el derecho de terceros, los propios de la organización, o bien para la realización de actos que pudieran ser considerados ilícitos.

7.2 RESPECTO A BASES DE DATOS FÍSICAS - NO AUTOMATIZADAS

- Guardar el necesario secreto respecto a cualquier tipo de información de carácter personal conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la entidad.

- Mantener debidamente custodiado el documento que lo identifica como empleado del Banco, así como las llaves de acceso, a sus oficinas y a los escritorios, archivadores u otros elementos que contenga bases de datos físicas - no automatizadas con datos de carácter personal, debiendo poner en conocimiento de su Gerente o líder, cualquier hecho que pueda comprometer esa custodia.

- Cerrar con llave los escritorios y las puertas de las oficinas al término de la jornada laboral o cuando deba ausentarse temporalmente de esta ubicación, a fin de evitar accesos no autorizados.

- Comunicar a la Gerencia de Privacidad, Ciberseguridad y Seguridad de la Información las incidencias de seguridad de las que tenga conocimiento asociadas a las bases de datos físicas.

- Queda prohibido el traslado de cualquier listado o documento análogo con datos de carácter personal en los que se almacene información de titularidad del Banco, fuera de las instalaciones de la misma, sin la autorización correspondiente.

- Guardar todos los soportes físicos o documentos que contengan información con datos de carácter personal en un lugar seguro, cuando estos no sean usados, particularmente fuera de la jornada laboral.

- Asegurarse de que no quedan documentos impresos que contengan datos protegidos impresos en la bandeja de salida de la impresora.

8 POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

Este numeral hace referencia a la Política publicada en internet, la cual comenzó a regir el 10 de octubre de 2015 y se encuentra a disposición de los clientes y usuarios por medio de la página web **www.bancopopular.com.co** y tiene como objetivo principal dar a conocer la regulación interna adoptada por el Banco en esta materia.

Las políticas de privacidad y protección de datos personales serán de aplicación a todas las Bases de Datos “automatizadas y físicas” que contengan Datos Personales que sean objeto de Tratamiento por parte de EL BANCO, incluida toda aquella información que haya sido obtenida o recolectada con anterioridad a la Ley 1581 de 2012 y cualquier otro dato que sea susceptible de ser tratado por el Banco en desarrollo de su objeto social o con ocasión de cualquier tipo de relación civil, laboral o comercial que llegue a surgir en virtud de sus actividades conexas o propias de su naturaleza societaria.

Las políticas y/o sus modificaciones son diseñadas por la Gerencia de Privacidad, Ciberseguridad y Seguridad de la Información y son aprobadas por la Gerencia Integral de Riesgo.

Estas son puestas en conocimiento de los titulares de la información a través de la página web de la entidad **www.bancopopular.com.co**.

El contenido principal de las políticas establece:

- Identificación del Responsable del tratamiento de datos personales.
- Nombre o razón social de la entidad.
- Alcance, aplicación y marco regulatorio.
- Finalidades y tratamiento de los datos personales.
- Autorización.
- Derechos que asisten a los titulares de la información personal.
- Persona o área responsable de la atención de peticiones, consultas y reclamos
- Canales de atención.
- Deberes de Banco Popular como Responsable y Encargado.
- Transferencia internacional de datos personales.

8.1 CAPTURA DE INFORMACIÓN

Para efectos de dar cumplimiento a lo dispuesto en el artículo 9 de la Ley 1581 de 2012, las áreas responsables de los canales por los que se vaya a solicitar datos personales, deberán establecerán mecanismos para obtener la autorización de los titulares o de quien se encuentrelo34 legitimado de conformidad con lo establecido en el artículo 2.2.2.25.4.1., del cap. 25 del Decreto 1074 de 2015, que garanticen su consulta.

Si la captura se hace en un medio físico, la autorización debe contar con la firma del titular de los datos; si se utiliza un medio tecnológico o verbal, se deben implementar mecanismos eficientes que permitan la conservación de su aceptación al tratamiento de los datos por parte de la entidad, y consulta cuando se requiera.

En los casos en que Banco Popular actúa como responsable de las bases de datos y sin importar el medio de captura, se debe obtener autorización del Titular de la información y guardar prueba de la misma.

8.2 AUTORIZACIONES

De conformidad con las normas vigentes, el consentimiento del Titular de los datos debe cumplir con las siguientes características:

- **Ser previo:** la autorización debe ser suministrada, en una etapa anterior a la incorporación del dato en la base de datos y a la utilización del mismo para fines comerciales.

- **Ser expreso:** Otorgarse de forma inequívoca, explícita y concreta para la finalidad que requiere.

- La autorización debe ser inequívoca, razón por la cual, no es posible aceptarse la existencia, dentro del ordenamiento jurídico colombiano, de un consentimiento tácito.

- **Ser informado:** El Titular del dato debe conocer la finalidad de la base de datos y el tratamiento que se le va a dar a sus datos; así como ser plenamente consciente de los efectos de su autorización. En concreto, es obligatorio informar al titular de los datos: (i) El tratamiento que se hará sobre sus datos y la finalidad del mismo; (ii) el carácter facultativo de las respuestas a las preguntas que versen sobre datos sensibles; (iii) los derechos que tiene; (iv) la identificación, dirección física o electrónica del responsable del tratamiento.

Para obtener la autorización se siguen las siguientes instrucciones:

En primer lugar, antes de que la persona autorice se le informará de forma clara y expresa lo siguiente:

- El tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo.

- El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de niñas, niños o adolescentes.

- Los derechos que le asisten como titular, previstos en el artículo 8 de la ley 1581 de 2012.

- La identificación, dirección y teléfono de Banco Popular**.**

- Los canales de atención del Banco para temas de tratamiento de datos**.**

En segundo lugar, se obtiene el consentimiento del titular a través de cualquier medio que pueda ser objeto de consulta posterior. Los mecanismos podrán ser predeterminados a través de medios técnicos que faciliten al titular su manifestación automatizada. Se entiende, como se indicó anteriormente, que la autorización cumple con estos requisitos cuando se manifiesta por:

- **Escrito:** Se deja prueba del cumplimiento de la obligación de informar y del consentimiento. Si el titular solicita copia, deberá suministrársele.

- **Verbalmente:** a través de llamadas telefónicas en las cuales el titular es informado de sus derechos y las finalidades de tratamiento de la información dándole la oportunidad a continuación de manifestar su aceptación. De dichas comunicaciones, se dejará prueba a través de grabaciones conservadas de manera que puedan ser objeto de posterior consulta.

- **Digital:** a través de aplicaciones y/o portales en internet, en los cuales el titular es informado de sus derechos y las finalidades de tratamiento de la información dándole la oportunidad a continuación de manifestar su aceptación. De dicha aceptación, se dejará prueba a través de reportes (logs) conservados de manera que puedan ser objeto de posterior consulta.

- **Conductas inequívocas del titular**: La autorización también puede obtenerse a partir de conductas inequívocas del Titular del Dato que permitan concluir de manera razonable que éste otorgó su consentimiento para el tratamiento de su información.

Cuando se trate de datos personales sensibles la autorización para el tratamiento de tales datos deberá hacerse de manera explícita. En ningún caso, el silencio del Titular podrá considerarse como una conducta inequívoca.

8.2.1 Casos en los que no es necesaria la autorización para el tratamiento de datos personales

La autorización del Titular no será necesaria cuando se trate de:

a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;

b) Datos de naturaleza pública;

c) Casos de urgencia médica o sanitaria;

d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;

e) Datos relacionados con el Registro Civil de las Personas.

Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la ley 1581 de 2012.

8.2.2 Autorización para tratamiento de datos sensibles

Banco Popular solo puede realizar operaciones o tratamientos de los datos sensibles con autorización previa y expresa del titular de dichos datos personales, siempre y cuando se haya informado al Titular:

Cuando se trate de la recolección de datos sensibles se deben cumplir los siguientes requisitos:

- La autorización debe ser explícita.
- Se debe informar al Titular que no está obligado a autorizar el tratamiento de dicha información.
- Se debe informar de forma explícita y previa al Titular cuáles de los datos que serán objeto de tratamiento son sensibles y la finalidad del mismo.

8.2.3 Autorización de tratamiento de datos de niños, niñas o adolescentes (NNA)

Cuando se trate de la recolección y tratamiento de datos de niños, niñas o adolescentes se deben cumplir los siguientes requisitos:

- La autorización debe ser otorgada por personas que estén facultadas para representar los NNA. El representante de los NNA deberá garantizarles el derecho a ser escuchados y valorar su opinión del tratamiento teniendo en cuenta la madurez, autonomía y capacidad de los NNA para entender el asunto.
- Se debe informar que es facultativo responder preguntas sobre datos de los NNA.
- El tratamiento debe respetar el interés superior de los NNA y asegurar el respeto de sus derechos fundamentales.
- Banco Popular solamente usará, almacenará y realizará tratamiento de datos personales de menores de edad que sean hijos, descendientes o que dependan o estén a cargo de los empleados o contratistas y que sean de naturaleza pública. La finalidad de dicho tratamiento será únicamente la de planear y realizar actividades relacionadas con el bienestar personal y familiar de los empleados y los menores.

8.3 AVISO DE PRIVACIDAD

El Banco Popular pone a disposición de los titulares el avisó de privacidad para el tratamiento de datos personales, este aviso es una comunicación verbal o escrita dirigida al Titular a través de medios físicos o electrónicos. A través de este documento se informa al Titular, la información relativa a la existencia de las políticas de tratamiento de información personal que le serán aplicables, la forma de acceder a dichas políticas y las características del Tratamiento que se pretende dar a los datos personales al momento de recolectar los datos personales.

A través de este documento se informa al Titular, la información relativa a la existencia de las políticas de tratamiento de información personal que le serán aplicables, la forma de acceder a dichas políticas y las características del Tratamiento que se pretende dar a los datos personales al momento de recolectar los datos personales.

El aviso de privacidad debe incluir como mínimo:

1. Nombre o razón social y datos de contacto del Responsable del Tratamiento.
2. El Tratamiento al cual serán sometidos los datos y la finalidad del mismo.
3. Los derechos que le asisten al Titular.
4. Los mecanismos dispuestos por el Responsable para que el Titular conozca la política de Tratamiento de la información y los cambios sustanciales que se produzcan en ella o en el Aviso de Privacidad correspondiente. En todos los casos, debe informar al Titular cómo acceder o consultar la política de Tratamiento de información.

8.4 PRUEBA DE LA AUTORIZACIÓN

Con el fin de que posteriormente se pueda consultar la autorización obtenida en medio físico, digital o magnetofónico (llamadas), el Banco conservará prueba de la misma, mientras el cliente se encuentre activo y posteriormente 10 años a partir de que deje de ser cliente del Banco, como soporte en posibles eventos que se puedan presentar contra el Banco.

Los Encargados de datos personales que actúan en dicha calidad con ocasión a un contrato de transmisión firmado con El Banco, están obligados a conservar las evidencias de las autorizaciones de tratamiento de datos personales entregadas por los titulares y capturadas a través de los diferentes mecanismos existentes. El Banco incluirá estas obligaciones en los contratos de protección de datos personales.

8.5 AUTORIZACION PARA EL TRATAMIENTO DE DATOS PERSONALES

Para realizar la actualización de la autorización de tratamiento de datos personales se debe tener en cuenta:

- El equipo jurídico de Grupo Aval es el encargado de definir y entregar la autorización para el tratamiento de datos personales a la Dirección de Estudios Jurídicos Institucionales del Banco, quien debe hacer el análisis y emitir el concepto del documento y comunicarlo a la Gerencia de Privacidad, Ciberseguridad y Seguridad de la Información.

- La personalización de la autorización para el tratamiento de datos personales para uso en el Banco es realizada por las áreas de la Dirección de Estudios Jurídicos Institucionales y la Gerencia de Privacidad, Ciberseguridad y Seguridad de la Información.

- Los canales propios habilitados para el ejercicio de derechos de los titulares son incluidos en la de autorización para el tratamiento de datos personales, una vez son informados por las Gerencias de Inteligencia de Negocios, Experiencia y Cuidado del Cliente, Segmentos y Canales, Gerencia de Operaciones Medios de Pago, Gerencia de Atención al Talento Humano en el caso de empleados y la Gerencia de Abastecimiento Estratégico para los casos de proveedores persona natural o arrendadores.

- La Gerencia de Privacidad, Ciberseguridad y Seguridad de la Información, comunica la versión actualizada de la autorización para el tratamiento de datos personales a las diferentes **áreas de producto**, **canales** y **filiales** del Banco, con el fin de que estás realicen las actualizaciones en los canales, formatos y documentos donde se tiene relacionada.

- Tener en cuenta que el tiempo para hacer la actualización de la autorización para el tratamiento de datos personales es de máximo 45 días calendario, a partir de la notificación enviada por la Gerencia de Privacidad, Ciberseguridad y Seguridad de la Información.

- Las áreas responsables de productos y de los canales en donde se presenta la autorización para el tratamiento de datos personales a los clientes, en procesos de enrolamiento, creación y actualización, deberán notificar a la Gerencia de Privacidad, Ciberseguridad y Seguridad de la Información, la fecha en la que efectivamente se implementó la autorización para el tratamiento de datos personales en los diferentes canales y formatos.

- Las áreas dueñas de formatos digitales en los cuales se encuentre incluida la cláusula de autorización para el tratamiento de datos personales, deberán solicitar a la Gerencia de Procesos y Automatización: el ajuste de los formatos, la

actualización en formas electrónicas y la socialización de estas novedades a través de un boletín.

- Las áreas dueñas de las formas electrónicas, que son impresas, deberán informar el cambio inmediatamente con el fin de que los formatos anteriores, en blanco se recojan y sean destruidos.

- Las áreas responsables de productos y canales, al igual que las filiales, deberán garantizar siempre la utilización de la última versión de la autorización para el tratamiento de datos personales avalada por la Dirección de Estudios Jurídicos Institucionales y la Gerencia de Privacidad, Ciberseguridad y Seguridad de la Información.

9 TRANSMISIÓN DE INFORMACIÓN

El intercambio o transmisión electrónica o física de datos personales se realiza de acuerdo a lo establecido en las Políticas y lineamientos de Seguridad de la Información implementados en Banco Popular.

Por lineamiento general se establece que:

- La información sensible, confidencial o privada que se transmita a través de las redes de telecomunicación tanto interna como externamente, debe ser protegida.

- Las áreas responsables de activos de información, con información sensible, confidencial o privada, deben definir qué controles de seguridad y privacidad se deben implementar para los servicios de red.

- Para la transmisión de información personal sensible de nivel de riesgo alto se deberán adoptar medidas de seguridad reforzadas.

- Previo a la transmisión de datos a terceros Encargados de datos personales, debe suscribirse previamente el contrato de transmisión de datos personales entre las partes.

10 TRANSFERENCIA Y TRANSMISIÓN DE DATOS A TERCEROS PAÍSES

Salvo autorización expresa del Titular de los datos personales y las demás excepciones previstas en la ley 1581 de 2012 está prohibida la transferencia de datos a terceros países que no proporcionen niveles adecuados de protección de datos.

10.1 TRANSMISIÓN DE DATOS A UN ENCARGADO PARA QUE HAGA EL TRATAMIENTO DE LOS DATOS PERSONALES:

Banco Popular podrá transmitir o entregar los datos personales de sus bases de datos a un tercero en Colombia o en el exterior para que este tercero, en calidad de encargado, realice el tratamiento de los datos personales. Para tales efectos y de conformidad con la ley, se deberá suscribir un contrato de transmisión de datos con dicho tercero en el que:

- Se señalará los alcances del tratamiento, las actividades que el encargado realizará para el tratamiento de los datos personales, las condiciones para el uso de los datos y las obligaciones del Encargado para con el titular y el responsable.

- El encargado se comprometerá a dar aplicación a las obligaciones bajo la Política de Tratamiento de la información y a realizar el Tratamiento de datos de acuerdo con la finalidad que los Titulares hayan autorizado y con las leyes aplicables.

- La Vicepresidencia Jurídica- Secretaría General, construirá los contratos de Transmisión o transferencia según sea el caso, y la Gerencia de Privacidad, Ciberseguridad y Seguridad de la información realizará la revisión, en conjunto se aprobará el documento.

11 ACCESO Y CONTROL DE LA INFORMACIÓN PERSONAL

La Vicepresidencia de Innovación Empresarial y la Gerencia de Tecnología deberán implementar los controles tecnológicos y de monitorización que permitan la trazabilidad y control de los usuarios que acceden a la información.

A nivel de instalaciones físicas y acceso a la documentación física no automatizada, cada una de las áreas será responsable por el acceso y control de la información que es mantenida en sus archivos de gestión

11.1 USO DE LA INFORMACIÓN

Los datos personales contenidos en las diferentes bases de datos serán usados y tratados únicamente para el fin establecido en las autorizaciones del titular.

Cualquier uso de la información diferente a la finalidad establecida previamente, debe ser incluido dentro de la autorización para el tratamiento de datos personales, la cual requerirá ser autorizada nuevamente por el titular con las finalidades adicionales.

Las nuevas finalidades a incorporar en la autorización de tratamiento de datos deberán ser validadas por la Vicepresidencia Jurídica – Secretaría General del Banco.

Únicamente los colaboradores autorizados podrán introducir, modificar o anular datos personales desde los aplicativos hacia las Bases de Datos, no está permitido ingresar datos directamente a la Base de Datos, en caso de requerirse se debe seguir lo establecido dentro de los lineamientos del modelo de Seguridad de la Información para adoptar las medidas oportunas sobre el mismo.

11.2 ALMACENAMIENTO DE INFORMACIÓN

El almacenamiento de la información automatizada y física se debe realizar en medios o ambientes que cuentan con adecuados controles para la protección de los datos. Esto involucra controles de seguridad, tecnológicos y de tipo ambiental en áreas restringidas, en instalaciones propias y/o centros de cómputo o centros documentales gestionados por terceros.

La custodia de la información deberá realizarse en condiciones que no causen el deterioro de los activos de información.

11.3 DESTRUCCIÓN

La destrucción de la información sobre datos personales contenida en medios físicos o electrónicos se realiza a través de mecanismos que no permiten su reconstrucción., de acuerdo con lo definido en la Directriz AVBP.DISI.GA.055 Destrucción de Información Reservada, del documento Directrices de Seguridad de la Información.

La destrucción de la información contenida en poder de terceros se debe realizar de acuerdo con lo definido a nivel contractual en la Cláusula Procedimientos y controles para la entrega y destrucción de la información.

12 GESTIÓN DE INCIDENTES RELATIVOS A BASES DE DATOS CON INFORMACIÓN PERSONAL

El Banco tiene establecido un procedimiento de gestión de incidentes de Privacidad con el fin de dar respuesta en caso de que un incidente pueda afectar o haber afectado a bases de datos con datos personales, este se deberá informar a la Gerencia de Privacidad, Ciberseguridad y Seguridad de la Información.

El Banco dispondrá de los recursos necesarios para brindar un apropiado monitoreo, detección y gestión de incidentes de Privacidad, estableciendo procedimientos para la gestión de los incidentes.

La responsabilidad de cada funcionario, contratista, colaborador o tercero es reportar de manera oportuna cualquier evento sospechoso, debilidad o violación de políticas que pueden afectar la privacidad de los titulares.

Todos los incidentes y eventos sospechosos deben ser reportados tan pronto como sea posible a través de los canales internos establecidos por Banco Popular en el proceso de RRI11 Gestión de Incidentes de Seguridad de la Información y Ciberseguridad. Los niveles de escalamiento en la comunicación ante un incidente de privacidad son los establecidos en el procedimiento mencionado anteriormente.

Los empleados deben reportar a su jefe directo y a la Gerencia de Privacidad, Ciberseguridad y Seguridad de la Información cualquier daño o pérdida de sus computadores o de cualquiera otro dispositivo que contenga información de empleados, clientes, o proveedores personas naturales.

A menos que exista una solicitud de la autoridad competente por un requerimiento administrativo judicial, ningún funcionario debe divulgar información sobre sistemas de cómputo, y redes que hayan sido afectadas por un delito informático o abuso de sistema. Para la entrega de información o datos en virtud de una orden de una autoridad, la Dirección de Apoyo Judicial de la Vicepresidencia Jurídica deberá intervenir con el fin de prestar el asesoramiento adecuado.

13 LINEAMIENTOS AL PROCEDIMIENTO DE ATENCIÓN DE DERECHOS DE LOS TITULARES

La Gerencia de Operaciones de Servicio al Cliente – PQR deberá incluir en sus procedimientos las acciones requeridas para atender oportunamente y bajo los lineamientos establecidos en la normativa vigente sobre protección de datos personales las consultas y reclamos.

El titular de la Información Personal suministrada a Banco Popular tendrá los siguientes derechos:

- Conocer, actualizar y rectificar su Información Personal gratuitamente.
- Solicitar prueba de la existencia de la autorización otorgada a Banco Popular.
- Ser informado respecto al uso que se le ha dado a su Información Personal.
- Revocar la autorización y solicitar la supresión del dato cuando no se haga un uso conforme a los usos y finalidades autorizados.
- Presentar consultas y reclamos referentes a la Información Personal.
- Los demás derechos consagrados en la ley.

13.1 DISPOSICIONES EN LOS PROCEDIMIENTOS DE CONSULTAS Y RECLAMOS

La solicitud de rectificación, actualización o supresión debe ser presentada a través de los medios habilitados por Banco Popular señalados en el presente documento, y contener, como mínimo, la siguiente información:

- El nombre, domicilio del titular y medio de contacto para recibir la respuesta como teléfono, correo electrónico, dirección de residencia.
- Los documentos que acrediten la identidad o la representación de su representante.
- La descripción clara y precisa de los datos personales respecto de los cuales el titular busca ejercer alguno de los derechos.
- En caso dado otros elementos o documentos que faciliten la localización de los datos personales.
- Evidencias del reclamo como mensajes de texto, correos electrónicos y cualquier otro documento soporte.

13.1.1 Consultas

Banco Popular garantiza el derecho de consulta, suministrando a las personas que actúen en ejercicio de este derecho, toda la información contenida en su registro individual o que esté vinculada con la identificación del titular. Las consultas y solicitudes deben ser dirigidas por el titular a través de cualquier medio y a cualquiera de los contactos que se señalan más adelante, y serán atendidas en un término máximo de diez (10) días hábiles, contados a partir de la fecha de recibo de las mismas por cualquier medio de comunicación. En caso de que no sea posible resolver la consulta dentro de este término, el titular será informado de dicha situación en la dirección de notificación que haya incluido en la respectiva consulta, y el término de respuesta se podrá extender hasta por cinco (5) días hábiles adicionales. La respuesta a las consultas o reclamos que el titular presente podrá ser entregada por cualquier medio físico o electrónico.

13.1.2 Reclamos

Cuando los titulares de la Información o sus causahabientes consideren que su información debe ser corregida, actualizada, suprimida, revocada la autorización, o cuando adviertan un presunto incumplimiento por parte de Banco Popular de sus deberes en materia de Protección de Datos Personales contenidos en la legislación aplicable y en la Política de Privacidad y Protección de Datos Personales, podrán presentar un reclamo de la siguiente manera:

- Presentar solicitud escrita frente al requerimiento específico.

- Si el reclamo resulta incompleto, Banco Popular requerirá al titular dentro de los cinco (5) días hábiles siguientes a la recepción de la solicitud para que complete y subsane su petición.
- Si transcurren dos (2) meses desde la fecha del requerimiento sin que el titular haya dado respuesta, se entenderá desistida la pretensión.
- Si quien recibe el reclamo no es competente para resolverlo, dará traslado a quien si lo sea para que resuelva en un término máximo de dos (2) días hábiles e informará de tal hecho al titular.
- Si el reclamo es recibido de manera completa o se ha completado posteriormente, deberá incluirse, dentro de los dos (2) días hábiles siguientes, una “leyenda” en la base de datos que indique “RECLAMO EN TRÁMITE”.
- Banco Popular resolverá el reclamo en un término máximo de quince (15) días hábiles contados a partir del día siguiente de recibo del mismo. En caso de que no sea posible resolver la consulta dentro de este término, el titular será informado de la demora, los motivos y la fecha de respuesta en la dirección de notificación que haya incluido en el respectivo reclamo. En todo caso, el término de respuesta no podrá superar de ocho (8) días hábiles siguientes al vencimiento del primer término. La respuesta al reclamo que el titular presente podrá ser efectuada por cualquier medio físico o electrónico.

13.1.3 Supresión del Dato

El titular tiene el derecho, en todo momento, a solicitar a Banco Popular, la supresión (eliminación) de sus datos personales cuando:

- Considere que los mismos no están siendo tratados conforme a los principios, deberes y obligaciones previstas en la Ley 1581 de 2012.
- Hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recolectados.
- Se haya superado el periodo necesario para el cumplimiento de los fines para los que fueron recolectados.
- La supresión del dato no procede cuando:
- El titular tenga un deber legal o contractual de permanecer en la base de datos.
- La eliminación de datos obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas.

- Los datos sean necesarios para proteger los intereses jurídicamente tutelados del titular; para realizar una acción en función del interés público, o para cumplir con una obligación legalmente adquirida por el titular.

- También debe tenerse en cuenta que en algunos casos cierta información deberá permanecer en registros históricos por cumplimiento de deberes legales de la organización por lo que su supresión versará frente al tratamiento activo de los mismos y de acuerdo a la solicitud del titular.

14 CANALES

Los canales habilitados para que los titulares y usuarios ejerzan sus derechos a conocer, actualizar, rectificar, suprimir datos y revocar la autorización son:

- Oficinas Bancarias a Nivel Nacional
- Llamando a nuestro Call Center en Bogotá D.C. al teléfono 60 -1- 743 4646 y resto del país, 01 8000 184646.
- Con relación a las consultas o reclamos de los colaboradores del Banco, estas deben ser dirigidas a la Gerencia de Atención y Servicios al Talento Humano mediante correo electrónico al buzón **geratencionsth@bancopopular.com.co**.
- Las consultas o reclamos de los proveedores personas naturales serán atendidas por la Gerencia de Abastecimiento Estratégico.

CONTROL DE CAMBIOS

HISTORIAL		
# VERSIÓN	**FECHA PUBLICACIÓN**	**DESCRIPCIÓN DEL CAMBIO**
1	26/06/2020	Se crea Política con el objeto de reglamentar los lineamientos del gobierno de datos personales, responsabilidades, conductas y disposiciones generales, enfocados en proteger la privacidad de los datos personales de clientes, empleados, proveedores, accionistas y demás personas naturales con las que el Banco tenga una relación.
2	6/10/2020	Se realiza la actualización de la política al incluir el ítem 7.4 Cláusula de Tratamiento de Datos Personales y cambia el nombre de la Gerencia de Riesgo No Financiero y Cumplimiento a Gerencia Oficial Corporativo de Riesgo (CRO) y del cargo Gerente de Riesgo No Financiero a Gerente Oficial Corporativo de Riesgo (CRO). Además se ajustan los canales de atención para los Titulares con el fin de que estén alienados con los definidos en la Política de Privacidad y Protección de Datos Personales ubicada en el Portal Web del Banco.
3	10/12/2021	Se realiza la actualización de la política: En el ítem 4.1.2 Forma de tratamiento se incluye como se deben registrar el inventario de la bases de datos personales ante la Superintendencia de Industria y Comercio En el ítem 5 Gobierno para la gestión de la privacidad se incluye el marco de referencia definida en el esquema de las tres líneas de defensa.
4	28/03/2023	Se actualizan los numerales 1 y 7, y se incorporan los numerales 6.1 y 8.2.1 de la presente política, con el fin de reglamentar el Programa Integral de Gestión de Protección de Datos