Política de Privacidad

Banco Internacional

En esta Política de Privacidad (en adelante, la "Política") se explica cómo Banco Internacional S.A. (en adelante el "Banco" o "Banco Internacional") realiza el tratamiento de datos personales, recolección, finalidad, base de licitud, comunicación, seguridad y los derechos que asisten a sus titulares, en todos sus canales de atención.

Esta Política debe interpretarse de manera complementaria a los contratos de productos y servicios del Banco o documentos accesorios.

Índice **1**

1. Introducción **2**
2. Alcance **2**
3. Marco Normativo Aplicable **2**
4. Responsable del Tratamiento y Canales de Contacto **3**
5. Categorías de Datos Personales Tratados **3**
6. Finalidades y Bases de Licitud del Tratamiento **4**
7. Conservación, Bloqueo, Eliminación y Anonimización **5**
8. Perfilamiento y Decisiones Automatizadas **6**
9. Uso de Cookies **6**
10. Ejercicio de los Derechos de los Titulares **7**
11. Fuentes de Procedencia de los Datos Personales **8**
12. Comunicación de Datos Personales, Destinatarios y Grupo Empresarial **8**
13. Encargados del Tratamiento y Proveedores **9**
14. Transferencias Internacionales de Datos Personales **9**
15. Videovigilancia, Grabaciones y Control de Acceso **10**
16. Seguridad de la Información y Confidencialidad **10**
17. Modificaciones y Vigencia **10**
18. Definiciones **11**

1. Introducción

El Banco reconoce que la protección de los datos personales constituye un derecho fundamental de las personas y un componente esencial de la confianza que debe existir en la actividad bancaria. En consecuencia, trata los datos personales de forma lícita, leal, transparente, segura y responsable, respetando los derechos de sus titulares y las exigencias legales y contractuales aplicables.

2. Alcance

Esta Política se aplica al tratamiento de datos personales realizado por el Banco en el contexto de los productos y servicios que ofrece a través de sus distintos canales de atención, abarcando las siguientes categorías de titulares personas naturales: clientes, potenciales clientes o interesados; usuarios de canales de atención digitales o telefónicos; avalistas, garantes y/o codeudores solidarios, representantes legales, apoderados, beneficiarios finales, proveedores y/o prestadores de servicios; accionistas, inversionistas o personas vinculadas a instrumentos financieros; postulantes, colaboradores o ex colaboradores; visitantes de oficinas o dependencias del Banco; y cualquier otra persona natural cuyos datos deban ser tratados por el Banco.

Esta Política no aplica al tratamiento de datos ni a las actividades realizadas por terceros que operen sitios web, aplicaciones, plataformas o servicios independientes del Banco bajo sus propios términos y finalidades, aun cuando existan enlaces, accesos o integraciones directas hacia ellos desde nuestros canales. En tales casos, el titular interactúa directamente con dichos terceros y deberá consultar sus respectivas políticas de privacidad y condiciones de uso.

3. Marco Normativo Aplicable

El Banco realiza el tratamiento de datos personales y la prestación de sus servicios en estricto cumplimiento de la Constitución Política de la República de Chile, las leyes, reglamentos e instrucciones de las autoridades e instituciones fiscalizadoras competentes en Chile, en todas aquellas materias aplicables a la actividad bancaria, protección de datos, seguridad de la información y cumplimiento normativo, conforme a sus textos vigentes o a las normas que en el futuro las modifiquen, complementen, reemplacen o entren en vigencia gradualmente. Para todos los efectos, la interpretación de estas disposiciones se realizará conforme a la legislación chilena aplicable.

4. Responsable del Tratamiento y Canales de Contacto

El responsable del tratamiento de los datos personales tratados a través de sus canales de atención es:

- **Razón Social:** Banco Internacional S.A.
- **Rol Único Tributario (RUT):** 97.011.000-3
- **Representante Legal:** Mario Chamorro Carrizo (C.I. 7.893.316-K)
- **Giro:** Empresa Bancaria autorizada y fiscalizada por la Comisión para el Mercado Financiero (CMF).

- **Domicilio Legal / Casa Matriz:** Avenida Apoquindo N° 6.750, piso 16, comuna de Las Condes, Santiago, Chile.
- **Sitio Web Oficial:** https://www.internacional.cl.

Adicionalmente, en cumplimiento del marco de responsabilidad proactiva (accountability) y gobierno corporativo, el Banco ha designado a un Delegado de Protección de Datos (DPO).

En caso de consultas o solicitudes relativas al tratamiento de sus datos personales, podrán dirigirse a protecciondedatos@internacional.cl u otros medios digitales que el Banco habilite para estos fines.

5. Categorías de Datos Personales Tratados

El Banco podrá tratar, a modo enunciativo y no limitativo, las siguientes categorías de datos personales en función del producto solicitado, canal utilizado, normativa aplicable y finalidad del tratamiento:

- **Identificatorios:** Atributos que permiten distinguir e individualizar formalmente a la persona, tales como nombre, número de cédula de identidad, fecha de nacimiento, ocupación, actividad económica, residencia tributaria y condición de persona políticamente expuesta (PEP), entre otros.
- **Contacto:** Información destinada a establecer comunicación con el titular, tales como domicilio, correo electrónico, teléfono fijo o móvil, dirección laboral y canal de atención preferente, entre otros.
- **Financieros, Contractuales, Transaccionales**: Información sobre la relación comercial, productos o servicios contratados, capacidad de pago, historial crediticio, origen de fondos, registro de operaciones, transferencias, movimientos y pagos, así como antecedentes y datos de terceros relacionados a la operación o contrato (apoderados, representantes, avales, codeudores o beneficiarios), entre otros.
- **Técnicos, Seguridad y Autenticación:** Datos recopilados durante la interacción en canales de atención presenciales o a distancia para verificar la identidad y resguardar la seguridad, incluyendo dirección IP, datos de dispositivo, registros de acceso, credenciales, datos asociados a factores de autenticación y registros de voz e imagen (grabaciones de llamadas o cámaras CCTV), entre otros.
- **Interacción con el cliente y datos inferidos:** Información generada en atenciones o deducida del comportamiento y relación con el Banco, tales como motivo y resolución de consultas o reclamos, respuestas en encuestas de satisfacción, perfiles de interés, segmentaciones comerciales y preferencias estimadas mediante modelos analíticos, entre otros.
- **Perfilamiento:** Información generada mediante análisis de datos para evaluar riesgos, scoring crediticio, prevención de fraudes y segmentación comercial, entre otros.
- **Sensibles:** Datos referidos a la esfera íntima o biológica del titular cuyo tratamiento requiere especial resguardo, tales como datos biométricos (patrón facial, huella dactilar, reconocimiento de voz, entre otros), situación socioeconómica, información relativa a la salud física o psíquica, así como antecedentes que revelen origen étnico

o racial, afiliación sindical, gremial o política, vida u orientación sexual e identidad de género, entre otros.

El Banco no solicitará datos que no sean necesarios para las finalidades informadas. Si el titular entrega voluntariamente datos no requeridos, el Banco podrá eliminarlos, realizar un bloqueo de acceso en los sistemas en caso que no sea posible eliminarlos, anonimizarlos o tratarlos únicamente cuando exista base de licitud suficiente y sea necesario para la gestión solicitada.

6. Finalidades y Bases de Licitud del Tratamiento

El Banco tratará datos personales únicamente para finalidades lícitas, específicas, informadas y compatibles con su actividad bancaria, financiera, comercial, operacional y tecnológica y en cumplimiento regulatorio, necesarios para evaluar solicitudes, celebrar o ejecutar contratos, cumplir obligaciones legales, prevenir fraudes, gestionar riesgos, atender exigencias regulatorias o proteger la seguridad de los titulares y del sistema financiero, considerando las siguientes bases de licitud:

- **Datos relativos a obligaciones de carácter económico, financiero, bancario o comercial:** El Banco tratará los datos personales vinculados a la existencia, cumplimiento, morosidad o extinción de obligaciones crediticias, financieras y comerciales del titular. Lo anterior, para evaluar solvencia económica, capacidad de pago y riesgo crediticio previo otorgamiento de productos financieros o servicios comerciales, monitorear el comportamiento financiero y transaccional para detectar anomalías y prevenir fraudes cibernéticos o bancarios, para generar reportes obligatorios y entregar información a los reguladores, gestionar procesos de cobranza y desarrollar modelos estadísticos internos y perfiles financieros automatizados para segmentar el nivel de riesgo.
- **Ejecución de contrato:** El Banco tratará los datos personales necesarios para celebrar, administrar, ejecutar, modificar o terminar productos y servicios contratados con el Banco, incluyendo la operación de cuentas, créditos, tarjetas, inversiones, seguros, canales digitales, atención de requerimientos, gestión de pagos, cobranza, cumplimiento de obligaciones contractuales y administración de la relación comercial vigente con el titular.
- **Medidas precontractuales:** El Banco tratará los datos personales necesarios para atender solicitudes previas a la contratación, tales como simular, cotizar, evaluar, preevaluar o preaprobar productos o servicios bancarios, financieros, crediticios, de inversión u otros ofrecidos por el Banco y requeridos por los clientes. Esta base de licitud permite tratar los datos personales necesarios para verificar antecedentes, validar identidad, analizar documentación, evaluar capacidad de pago, riesgo crediticio, elegibilidad y condiciones comerciales, con el objeto de responder la solicitud del titular antes de la eventual contratación.
- **Obligación legal o regulatoria:** El Banco tratará datos personales que sean necesarios para dar cumplimiento a la legislación y normativa vigente, como para dar cumplimiento a las normas relativas a la prevención de delitos financieros, responder requerimientos y/o cumplir instrucciones de autoridades u organismos competentes;

asimismo atender exigencias propias de la regulación y fiscalización de la actividad bancaria.

- **Interés legítimo:** El Banco tratará datos personales necesarios para fines legítimos del Banco o de terceros, tales como prevención de fraude, seguridad de la información, mejora de servicios, control interno, seguridad física de los activos y las personas, auditoría o análisis estadístico, siempre que no prevalezcan los derechos y libertades del titular.
- **Defensa y ejercicio de derechos ante organismos de la administración pública y/o tribunales de justicia:** El Banco tratará los datos personales necesarios para la interposición de acciones judiciales o para su defensa en procedimientos de la misma naturaleza, y para la interposición o intervención en procedimientos ante autoridades administrativas.
- **Consentimiento:** El Banco tratará los datos personales respecto de los que se haya otorgado consentimiento de manera previa, libre, informada y específica, tales como, enviar comunicaciones comerciales personalizadas, las cookies opcionales, tratamientos de datos sensibles cuando la ley exige autorización expresa informadas al titular.

Extinguidas las finalidades que autorizan el tratamiento, el Banco procederá a la eliminación o anonimización de la información conforme a las reglas descritas en la sección siguiente.

7. Conservación, Bloqueo, Eliminación y Anonimización

El Banco conservará los datos personales únicamente durante el tiempo necesario para cumplir las finalidades que motivaron su recolección y para mantener la continuidad operacional de sus servicios, salvo que la legislación aplicable exija o indique plazos de conservación distintos.

Los plazos de conservación se determinarán en función de los siguientes criterios:

- Durante la vigencia de la relación contractual, precontractual o comercial con el titular.
- Cumplimiento de plazos legales de almacenamiento exigidos por la Ley General de Bancos, la CMF, normativa tributaria y de prevención de delitos financieros.
- Atención de reclamos, auditorías, procesos judiciales, fiscalizaciones o plazos de prescripción de acciones legales.
- Resguardo de evidencia de autorizaciones, transacciones, medidas de ciberseguridad y registros de auditoría.

Una vez cumplidas las finalidades y transcurridos los plazos legales o contractuales de resguardo, el Banco procederá a la eliminación o anonimización irreversible de los datos. En caso de que la eliminación técnica no sea inmediata debido a procesos automáticos de respaldo o sistemas de continuidad, la información se mantendrá bloqueada y con acceso restringido hasta su depuración definitiva o anonimización irreversible.

8. Perfilamiento y Decisiones Automatizadas

El Banco podrá utilizar herramientas analíticas, reglas automatizadas, modelos estadísticos, inteligencia artificial, machine learning, motores de decisión, scoring, alertas transaccionales o tecnologías similares para apoyar procesos bancarios, comerciales, de seguridad, cumplimiento y gestión de riesgos.

Estos tratamientos pueden emplearse, entre otros, para:

- Evaluar riesgo crediticio, capacidad de pago y comportamiento financiero.
- Detectar operaciones inusuales, fraudes, suplantaciones o patrones incompatibles con el uso normal de productos.
- Cumplir obligaciones regulatorias, monitoreo transaccional y prevención de lavado de activos.
- Personalizar la experiencia de usuario, priorizar atención, proponer productos o beneficios y mejorar canales digitales.
- Segmentar comunicaciones, siempre respetando el derecho de oposición y las reglas aplicables a marketing.
- Mejorar controles de ciberseguridad, autenticación, prevención de accesos indebidos y continuidad operacional.

Cuando una decisión basada exclusivamente en tratamiento automatizado produzca efectos jurídicos o afecte significativamente al titular, el Banco aplicará las garantías exigidas por la ley. Entre ellas el titular podrá solicitar información clara sobre la lógica general del tratamiento, posibilidad de solicitar revisión humana, impugnar la decisión, solicitar la corrección de datos inexactos y ejercicio de los demás derechos aplicables.[1]

9. Uso de Cookies

El Banco utiliza cookies, identificadores de dispositivo, registros técnicos y tecnologías similares estrictamente necesarias para operar sus canales digitales, mantener la disponibilidad del servicio, realizar balanceo de carga, asegurar la trazabilidad técnica de las sesiones, prevenir accesos no autorizados, detectar comportamientos anómalos, mitigar riesgos de fraude o ciberseguridad y resguardar la continuidad y seguridad de la navegación. Dentro de esta categoría podrán emplearse tecnologías propias o de terceros que presten servicios tecnológicos al Banco, tales como soluciones de seguridad, disponibilidad y balanceo. Estas tecnologías son indispensables para el funcionamiento seguro del sitio o aplicación, por lo que se mantendrán activas aun cuando el titular rechace cookies opcionales.

El Banco además puede utilizar cookies opcionales, por lo que únicamente se activarán si el titular otorga previamente su consentimiento, pudiendo modificarse o rechazarse en cualquier momento sin afectar el uso del sitio. Estas cookies son:

- De análisis o analíticas: Se utilizan para comprender cómo interactúan los usuarios en sus canales digitales, evaluar su funcionamiento y mejorar continuamente la experiencia de navegación. Utilizan datos tales como datos de la sesión, datos técnicos del dispositivo y comportamiento en el sitio.

[1] Derecho exigible conforme a la entrada en vigencia de la Ley N° 21.719

- De marketing, publicidad y redes sociales: Para medir la efectividad de sus campañas y ofrecer anuncios, promociones o contenidos de interés en plataformas digitales. Utilizan datos tales como interacciones comerciales específicas, identificadores publicitarios, vinculación con redes sociales, entre otros.

10. Ejercicio de los Derechos de los Titulares

Los titulares, de acuerdo a la legislación vigente, mantienen derechos de acceso, rectificación, cancelación/supresión y oposición. Además de los derechos de portabilidad, bloqueo y de impugnación de decisiones automatizadas que produzcan efectos jurídicos o le afecten significativamente.[2]

Para ejercer estos derechos, el titular deberá enviar una solicitud al correo derechosarco@internacional.cl o utilizar otros canales habilitados por el Banco. La solicitud debe permitir identificar claramente al titular, el derecho que desea ejercer, los datos o tratamiento al que se refiere, el medio para recibir respuesta y los antecedentes que respalden la solicitud cuando sea necesario.

El Banco podrá solicitar información adicional que sea necesaria para verificar la identidad del solicitante o la representación de quien actúe por cuenta del titular. Esta verificación busca proteger al titular.

El Banco responderá dentro de los plazos establecidos por la normativa vigente.

Se hace presente que la oposición al tratamiento para fines publicitarios o de marketing no afectará a las comunicaciones que el Banco deba enviar por obligación legal o contractual.

Para garantizar la seguridad de la información y la efectividad de sus derechos, el titular debe garantizar que la información entregada al Banco sea verídica, exacta y completa, informando oportunamente cualquier cambio relevante, resguardar de forma estrictamente personal y no compartir con terceros sus claves, credenciales, dispositivos o factores de autenticación, informar al Banco a la brevedad ante cualquier sospecha de fraude, uso indebido de credenciales o accesos no autorizados y no proporcionar datos personales de terceras personas sin contar con la autorización legal o el mandato expreso para realizarlo. La entrega de información falsa, incompleta o errónea facultará al Banco para suspender, rechazar o dejar sin efecto cualquier solicitud de producto o proceso de evaluación, sin perjuicio de las responsabilidades civiles o penales que pudieran originarse conforme a la legislación vigente.

11. Fuentes de Procedencia de los Datos Personales

El Banco recopila y trata datos personales obtenidos a través de las siguientes fuentes:

- Fuentes directas cuando los datos personales son proporcionados por el propio titular, ya sea mediante formularios de apertura y postulación, datos derivados de la relación precontractual o contractual y transaccional o mediante los canales de servicio del Banco.

[2] Aquellos que sean exigibles conforme a la entrada en vigencia de la Ley N° 21.719.

- Fuentes indirectas cuando los datos personales se obtienen a través de terceros o registros autorizados, como las fuentes de acceso público y registros oficiales (Registro Civil, Diario Oficial, Poder Judicial, entre otros), fuentes crediticias, comerciales y burós de crédito.
- Fuentes automatizadas, tecnológicas e inferidas, como lo son la geolocalización y biometría, navegación digital y modelos de perfilamiento.

12. Comunicación de Datos Personales, Destinatarios y Grupo Empresarial

El Banco no vende ni comercializa bases de datos personales. La comunicación o cesión de datos personales a terceros procederá únicamente cuando exista una base de licitud y se realizará bajo estrictos deberes de confidencialidad, seguridad y finalidad.

El Banco podrá comunicar datos personales a las siguientes categorías de destinatarios:

- **Autoridades e Instituciones Públicas:** Organismos regulatorios, judiciales, tributarios, policiales o fiscalizadores competentes (tales como Comisión para el Mercado Financiero, Unidad de Análisis Financiero, Servicio de Impuestos Internos, Banco Central de Chile, tribunales de justicia y Ministerio Público).
- **Filiales y Grupo Empresarial:** Empresas filiales Baninter Corredores de Seguros Limitada (RUT 76.002.878-9), Autofin S.A. (RUT 76.139.506-8) y Banco Internacional Administradora General de Fondos S.A. (RUT 76.930.984-5), así como empresas relacionadas al grupo empresarial al que pertenece el Banco, incluidas, mas no limitadas a, Inversiones la Construcción S.A. - RUT 94.139.000-5, Compañía de Seguros Confuturo S.A. - RUT 96.571.890-7, Compañía de Seguros Vida Cámara S.A. - RUT 99.003.000-6, Empresas Red Salud S.A. - RUT 76.020.458-7, y demás entidades informadas en el Registro de Grupos Empresariales de la CMF, en el link https://www.cmfchile.cl/institucional/estadisticas/registro_grupos_empresariales.php
- **Participantes del Sistema Financiero y Contrapartes:** Sociedades de apoyo al giro, corresponsales, operadores de tarjetas, marcas de pago, cámaras de compensación, aseguradoras, entidades de cobranza y contrapartes necesarias para ejecutar las operaciones solicitadas.
- **Proveedores de Servicios y Encargados:** Terceros que prestan servicios tecnológicos, soporte, auditoría, custodia u operación por cuenta del Banco, conforme a las reglas fijadas en la cláusula siguiente.
- **Burós de Crédito y Asesores:** Registros de información comercial conforme a la ley, así como auditores externos, clasificadoras de riesgo y asesores legales o consultores.

La información protegida por las reglas de secreto y reserva bancaria establecidas en la Ley General de Bancos sólo será cedida cuando sea autorizada explícitamente por el cliente, requerida por autoridad competente o permitida expresamente por la legislación vigente.

13. Encargados del Tratamiento y Proveedores

Cuando un tercero o proveedor requiera acceder o tratar datos personales por cuenta del Banco en calidad de mandatario o Encargado del Tratamiento, dicho procesamiento se

formalizará mediante acuerdos contractuales de protección de datos y confidencialidad. Los proveedores deberán actuar exclusivamente bajo las instrucciones documentadas del Banco, sin eximir a este último de su responsabilidad como responsable del tratamiento.

Según la criticidad y riesgo del servicio, el Banco exigirá a sus proveedores al menos las siguientes condiciones contractuales y operativas:

- **Finalidad y Reserva:** Deber de confidencialidad y prohibición absoluta de utilizar los datos para fines propios o comunicarlos a terceros no autorizados.
- **Medidas de Seguridad:** Implementación de controles técnicos, organizativos y físicos adecuados para garantizar la confidencialidad, integridad y disponibilidad de la información, incluyendo control de accesos, trazabilidad y gestión de vulnerabilidades.
- **Incidentes y Subcontratación:** Obligación de notificar incidentes de seguridad sin dilación indebida y sujetar la subcontratación o subencargados a las reglas del Banco.
- **Término del Servicio y Auditoría:** Eliminación o devolución segura de los datos al finalizar el contrato y facultad del Banco para auditar o verificar el cumplimiento de estas obligaciones.
- **Cumplimiento Normativo:** Observancia estricta de las normas de la CMF en materia de externalización de servicios, seguridad de la información, ciberseguridad y continuidad operacional.

14. Transferencias Internacionales de Datos Personales

El Banco podrá transferir, procesar, almacenar o permitir el acceso remoto a datos personales desde el extranjero cuando resulte necesario para la prestación de servicios bancarios, uso de infraestructura tecnológica o servicios en la nube, procesamiento de pagos internacionales, corresponsalía, soporte técnico, ciberseguridad, prevención de fraudes o cumplimiento regulatorio.

Toda transferencia internacional de datos se sujetará a los requisitos legales vigentes y requerirá la aplicación de salvaguardas y medidas de resguardo adecuadas, tales como:

- Cláusulas contractuales de protección de datos, confidencialidad, seguridad, regulación de incidentes y retorno o eliminación de la información.
- Medidas técnicas de resguardo, como cifrado de datos en tránsito y reposo, control de accesos y registros de auditoría.
- Respeto continuo de las normas de secreto y reserva bancaria y de las exigencias dictadas por la CMF sobre procesamiento de datos y ciberseguridad en el exterior.
- Información al titular de los datos en los casos en que la legislación aplicable lo exija.

15. Videovigilancia, Grabaciones y Control de Acceso

El Banco utiliza cámaras de seguridad, grabación de llamadas, y otros mecanismos similares para proteger personas, bienes, instalaciones, operaciones, seguridad bancaria, prevención de ilícitos, atención de clientes, respaldo de instrucciones, calidad de servicio, cumplimiento normativo y defensa de derechos.

El Banco informará la existencia de videovigilancia u otros registros mediante avisos visibles, mensajes de audio, cláusulas contractuales u otros medios razonables. Las grabaciones se conservarán por el plazo necesario para cumplir su finalidad y los plazos legales o regulatorios aplicables.

16. Seguridad de la Información y Confidencialidad

Ningún sistema es absolutamente invulnerable; sin embargo, el Banco despliega sus mejores esfuerzos para implementar medidas de seguridad técnicas, físicas, de gobierno y organizacionales, contractuales, de acceso, continuidad operacional y cualquier medida razonable y proporcional para prevenir, detectar, contener y responder a incidentes, conforme a la normativa aplicable y a los estándares de la industria bancaria, orientadas a proteger los datos personales frente a destrucción, pérdida, filtración, alteración, acceso no autorizado, uso indebido o indisponibilidad de sus servicios. Estas medidas se aplican bajo un enfoque basado en riesgos y consideran la naturaleza de los datos, la finalidad del tratamiento, la probabilidad e impacto de incidentes y las exigencias regulatorias aplicables a entidades bancarias.

En el caso de la ocurrencia de incidentes que puedan afectar datos personales, el Banco cuenta con procedimientos que detallan las siguientes etapas: detección, clasificación, contención, erradicación, recuperación, investigación, análisis de causa raíz, evaluación de impacto, registro, comunicación interna, notificación a autoridades o titulares cuando proceda, medidas correctivas y mejora continua.

El Banco no se hace responsable por interrupciones derivadas de caídas generales de telecomunicaciones, ataques distribuidos de denegación de servicio (DDoS) ajenos a su control razonable o ventanas programadas de mantenimiento técnico preventivo.

17. Modificaciones y Vigencia

El Banco podrá modificar esta Política para adaptarla a cambios legales, regulatorios, tecnológicos, operacionales, contractuales, de seguridad, de negocio o de mejores prácticas. La versión vigente estará disponible en el sitio web institucional y, cuando corresponda, en aplicaciones móviles u otros canales digitales del Banco.

Cuando los cambios sean sustanciales y la ley lo exija, el Banco informará a los titulares mediante mecanismos razonables, tales como publicación destacada en el sitio web, notificaciones en canales digitales, correo electrónico, mensajes en aplicaciones, comunicaciones contractuales u otros medios disponibles.

18. Definiciones

Para evitar ambigüedades, los siguientes conceptos tendrán el significado que se indica. Si la legislación vigente define un concepto de manera distinta o más precisa, prevalecerá la definición legal aplicable.

- **Canales de atención:** Todos los entornos, plataformas, medios o puntos de contacto (presenciales o a distancia) habilitados por el Banco para la interacción, consulta,

gestión, evaluación, contratación, operación o prestación de productos y servicios a los titulares. Comprende, de forma enunciativa y no limitativa:

  - Presenciales o Físicos: Sucursales, oficinas comerciales, casa matriz y demás dependencias físicas del Banco.
  - Digitales y Remotos: Sitios web oficiales, aplicaciones móviles, banca en línea, portales de clientes, formularios web, chat, redes sociales, mensajería electrónica, APIs e integraciones tecnológicas de atención remota.
  - Telefónicos y Telemáticos: Call center, sistemas de respuesta de voz interactiva (IVR), líneas de atención telefónica, videollamadas y cualquier otro medio o tecnología de comunicación a distancia basada en voz o datos.

- **Cookies y Tecnologías Similares:** Archivos o identificadores almacenados o consultados en el dispositivo del usuario al navegar por los sitios web o aplicaciones del Banco, destinados a permitir el funcionamiento técnico del canal, recordar preferencias, medir el rendimiento y reforzar la seguridad.
- **Incidente o Violación de Seguridad de Datos:** Evento que ocasiona o puede ocasionar la destrucción, pérdida, alteración, filtración, acceso no autorizado o indisponibilidad accidental o ilícita de datos personales.
- **Medidas de Seguridad:** Conjunto de controles organizativos, técnicos, de acceso, continuidad operacional y resguardo físico destinados a garantizar la confidencialidad, integridad y disponibilidad de los datos personales. Comprende:

  - Gobierno y organización: Políticas internas, segregación de funciones, capacitaciones y auditorías.
  - Controles de acceso: Autenticación, autorización, perfilamiento y mínimos privilegios.
  - Seguridad técnica: Cifrado, antimalware, protección de redes, monitoreo y gestión de vulnerabilidades.
  - Continuidad y resiliencia: Respaldos, planes de recuperación ante desastres y pruebas de disponibilidad.
  - Seguridad física: Control de accesos a dependencias, registro de visitas y monitoreo por cámaras CCTV.