



**ASOCIACIÓN BANCARIA
DE PANAMÁ**

GUÍA DEL DPO SEGÚN EL ACUERDO NO. 001-2022

Comisión de Protección de Datos

Tabla de contenido

Sección 1. Aspectos Generales	6
1. ¿Cuál es el ámbito de aplicación del acuerdo? (Art.1).....	6
2. ¿Cuál es el objetivo del acuerdo? (Art. 2)	6
3. ¿Cuál es el alcance y enfoque del acuerdo? (Art. 3).....	6
4. ¿Qué términos y definiciones son relevantes para entender el acuerdo? (Art. 4)....	6
Sección 2. Principios y Derechos para la Protección de Datos Personales	8
5. ¿Cuáles son los principios generales de protección de datos personales? (Art. 5).	8
6. ¿En qué consiste el principio de transparencia? (Art. 6)	10
7. ¿Qué significa el principio de licitud a través del consentimiento? (Art. 7).....	10
8. ¿Cuáles son los derechos ARCOP (Acceso, Rectificación, Cancelación, Oposición, Portabilidad)? (Art. 8 y 9)	11
Sección 3. Tratamiento de Datos Personales	14
9. ¿Cuáles son las condiciones y formalidades para el tratamiento de datos personales? (Art. 10)	14
10. ¿Qué es un aviso de privacidad y qué debe contener? (Art. 11)	17
11. ¿Cómo se manejan los datos personales obtenidos de otras fuentes? (Art. 12) ...	21
12. ¿Qué tratamientos de datos personales no requieren del consentimiento del titular? (Art. 13)	23
13. ¿Quiénes son los custodios de bases de datos y cuáles son sus responsabilidades? (Art.14)	25
14. ¿Cómo se debe llevar el registro de transferencias de datos personales? (Art. 15)	27
15. ¿Qué procedimientos deben seguirse para la conservación de datos personales? (Art. 16)	31
16. ¿Cuándo y cómo realizar una evaluación de impacto en el tratamiento de datos personales? (.....)	32
<i>A continuación, tabla con ejemplos de cuando aplicar la evaluación de impacto:</i>	
Sección 4. Gestión de los Datos Personales	35
17. ¿Cómo debe ser el sistema de control interno para la gestión de datos personales? (Art. 17)	35
18. ¿Cuáles son las responsabilidades de la junta directiva en la protección de datos personales? (Art. 18)	36

19. ¿Qué implica la certificación de cumplimiento de la junta directiva? (Art. 19).....	37
20. ¿Qué funciones tiene la unidad de administración de riesgo en relación con la protección de datos personales? (Art. 20).....	38
21. ¿Cómo se realiza la auditoría interna y el seguimiento del sistema de control interno? (Art. 21)	39
22. ¿Qué debe considerar la entidad bancaria cuando designa al Oficial de Protección de Datos? (Art. 22).....	41
23. ¿Cuáles son las funciones específicas del oficial de protección de datos (OPD)? (Art. 23).....	44
Sección 5. Tratamiento y Transferencia de los Datos Personales.....	47
24. ¿Qué medidas técnicas y organizativas deben adoptarse para el tratamiento de datos personales? (Art. 24).....	47
25. ¿Cómo se garantiza la seguridad en el tratamiento de datos personales? (Art. 25)	48
26. ¿Qué acciones deben tomarse ante un incidente de seguridad de datos personales? (Art. 26).....	50
Sección 6. Formación y Capacitación.....	51
27. ¿Cómo debe ser la capacitación del oficial de protección de datos y su equipo? (Art. 23)	51
28. ¿Qué debe incluir el programa de capacitación a colaboradores?	52
29. ¿Es necesario realizar las campañas de sensibilización a clientes, colaboradores y proveedores.....	54
Sección 7. Disposiciones Finales.....	55
30. ¿Cómo se gestionan los reclamos ante la Superintendencia? (Art. 27)	55
31. ¿Cuál es el procedimiento de seguimiento, control y supervisión del acuerdo? (Art. 28)	58
32. ¿Qué sanciones pueden aplicarse en caso de incumplimiento del acuerdo? (Art. 29)	59
33. ¿Cuándo entra en vigor el acuerdo y cuáles son sus disposiciones de vigencia? (Art. 30)	60
ANEXOS	62
Anexo 1 - Hoja de ruta sugerida para el cumplimiento de la Ley 81, su reglamentación y el acuerdo 01-2022	62
Anexo 2 - Artículo 15. Registro de transferencia de datos.	63
Anexo 3. Aviso de Privacidad.....	66



Anexo 4. Ficha Técnica / Manual de Protección de Datos	68
Anexo 5. Casos de uso / Consultas generales	69
<i>Caso de Uso 1</i>	69
<i>Caso de Uso 2</i>	69
<i>Caso de Uso 3</i>	69
<i>Caso de Uso 4</i>	70
<i>Caso de Uso 5</i>	70
<i>Caso de Uso 6</i>	71
<i>Caso de Uso 7</i>	71
<i>Caso de Uso 8</i>	72
<i>Caso de Uso 9</i>	72
Anexo 6. Matriz de Riesgos de Protección de datos	74
Participantes de la Comisión de Protección de Datos Personales	76
Referencias	76

INTRODUCCIÓN

Esta guía ha sido creada con la finalidad de orientar a todos los Oficiales de protección de datos del sector bancario, en cómo implementar dentro de sus organizaciones la normativa referente a protección de datos personales, recomendaciones para definir su estrategia de protección de datos y planes de acción, revisión y supervisión.

Dentro del presente documento se han desarrollado los artículos del acuerdo 001-2022, normativa especializada para el sector bancario en materia de protección de datos, la cual se desprende de la Ley 81 del 26 de marzo de 2019 sobre protección de datos personales y su reglamentación a través del Decreto Ejecutivo 285 del 28 de mayo de 2021.

En este documento usted encontrará lo siguiente:

- *Interpretación del artículo*
- *Recomendación de cómo implementarlo.*
- *Sugerencias de texto o modelos (en los casos que aplique).*

Los conceptos, interpretaciones y recomendaciones desarrollados a lo largo de la presente guía, son el resultado de una serie de reuniones celebradas por una mesa técnica conformada por miembros de la Comisión de Protección de Datos de la Asociación Bancaria de Panamá.

Cada institución establecerá la estrategia de implementación que se ajuste sus necesidades y las capacidades de la entidad bancaria siempre enfocada en cubrir todo lo que pide el régimen de protección de datos en Panamá.

Sección 1. Aspectos Generales

1. ¿Cuál es el ámbito de aplicación del acuerdo? (Art.1)

Como nuevo Oficial de Protección de Datos (DPO), es crucial que entiendas el ámbito de aplicación del Acuerdo No. 001-2022. Este acuerdo se aplica a todas las entidades bancarias que operan en Panamá, tal como se detalla en el Artículo 1. En tu rol, debes asegurarte de que la entidad bancaria cumpla con los principios, derechos y obligaciones establecidos para la protección de datos personales. Esto incluye la gestión, tratamiento y transferencia de información de los clientes, garantizando siempre su confidencialidad, integridad y disponibilidad. Cumplir con este acuerdo es fundamental para proteger los datos personales y mantener la confianza de nuestros clientes.

2. ¿Cuál es el objetivo del acuerdo? (Art. 2)

El Artículo 2, tiene como propósito establecer protocolos, procesos y procedimientos específicos para el tratamiento, transferencia y custodia de datos personales dentro de las entidades bancarias. Tu responsabilidad será asegurarte de implementar estos lineamientos para proteger los derechos de los clientes en relación con sus datos personales. Esto incluye garantizar que todas las prácticas de manejo de datos cumplan con los estándares de seguridad y privacidad, promoviendo así la confianza y transparencia en todas las operaciones bancarias.

3. ¿Cuál es el alcance y enfoque del acuerdo? (Art. 3)

El Acuerdo No. 001-2022 se aplica a todas las entidades bancarias en Panamá y establece lineamientos mínimos para la protección de datos personales de los clientes. El enfoque es garantizar la protección de los datos personales, independientemente de la nacionalidad o residencia del cliente, y abarcar tanto a las entidades bancarias como a sus custodios de bases de datos y proveedores de servicios relacionados.

4. ¿Qué términos y definiciones son relevantes para entender el acuerdo? (Art. 4)

Como parte fundamental, es esencial que te familiarices con los términos y definiciones clave establecidas en el Artículo 4 del Acuerdo No. 001-2022. Aquí tienes los términos más relevantes para entender y aplicar correctamente el acuerdo:

1. Almacenamiento de datos: Conservación o custodia de los datos personales del cliente en una base de datos, utilizando cualquier medio, incluido el tecnológico.
2. Aviso de privacidad: Comunicación dirigida al cliente para informarle sobre el tratamiento de sus datos personales, sus características y finalidades.
3. Base de datos: Conjunto organizado de datos personales que permite su tratamiento o transmisión.
4. Cliente: Persona natural titular de los datos personales que adquiere un servicio o producto bancario, o que se encuentra en la fase previa de adquisición.
5. Consentimiento: Manifestación de la voluntad libre, específica, informada e inequívoca del titular de los datos para su tratamiento.
6. Custodio de la base de datos: Persona natural o jurídica que, en nombre de la entidad bancaria, custodia la base de datos y los datos personales en ella contenidos.
7. Dato personal: Cualquier información que identifica o hace identificable a una persona natural.
8. Derechos ARCO: Derechos de acceso, rectificación, cancelación, oposición y portabilidad de los datos personales.
9. Proveedor de servicios bancarios: Persona natural o jurídica contratada por el banco para realizar actividades vinculadas con el negocio bancario y que está involucrada en el tratamiento de datos personales.
10. Responsable del tratamiento de los datos: Entidad bancaria que decide sobre el tratamiento de los datos personales y determina sus fines, medios y alcance.
11. Titular de los datos: Persona natural a la que se refieren los datos personales.
12. Tratamiento de datos: Cualquier operación sobre datos personales, como recolección, almacenamiento, organización, modificación, uso, transferencia o eliminación.

Comprender estos términos es fundamental para interpretar y aplicar correctamente las políticas y procedimientos relacionados con la protección de datos personales en su entidad bancaria.

NOTA: Como parte de estas definiciones recuerda revisar las definiciones del Decreto Ejecutivo 285, artículo 4.

Sección 2. Principios y Derechos para la Protección de Datos Personales

5. ¿Cuáles son los principios generales de protección de datos personales? (Art. 5)

Como nuevo Oficial de Protección de Datos (DPO), es crucial implementar y supervisar la aplicación de estos principios generales de protección de datos personales en nuestra entidad bancaria. Aquí te detallo los pasos a seguir:

1 Lealtad Garantizar que el tratamiento de datos sea justo, legal y sin engaños ni malas prácticas.	2 Finalidad Uso de datos solo solo para fines claros y legítimos.	3 Proporcionalidad Evita recolectar datos innecesarios. Usar solo los datos necesarios, sin excesos.
4 Veracidad y Exactitud Verificar y mantener los datos personales correctos y actualizados	5 Seguridad de los Datos Proteger la información contra accesos no autorizados.	6 Transparencia Informar a los titulares sobre el uso de sus datos.
7 Confidencialidad Asegurar que los datos sean protegidos y no divulgados	8 Licitud Procesar datos solo con una base legal válida.	9 Portabilidad Permitir a los titulares transferir sus datos a otra entidad

1. **Lealtad:** Asegúrate de que todos los tratamientos de datos se realicen de manera justa y legal, sin engaños ni malas prácticas y conforme a la normativa vigente.
2. **Finalidad:** Define claramente los fines específicos, explícitos y legítimos para los cuales se recolectan los datos personales y asegúrate de que todos los empleados los conozcan y respeten.
3. **Proporcionalidad:** Limita la recolección y el tratamiento de datos solo a lo necesario para los fines establecidos. Evita recolectar datos innecesarios.
4. **Veracidad:** Implementa procedimientos para verificar y mantener la exactitud de los datos personales, incluyendo la rectificación o eliminación de datos inexactos.
5. **Exactitud:** Establece mecanismos para la corrección de datos inexactos y asegúrate de que los datos se mantengan actualizados.

6. Seguridad de los datos: Implementa medidas técnicas y organizativas adecuadas para proteger los datos personales contra accesos no autorizados, pérdida o destrucción.
7. Transparencia: Desarrolla y comunica políticas de privacidad clara y accesible. Informa a los titulares sobre cómo y por qué se están tratando sus datos personales.
8. Confidencialidad: Asegura que todos los empleados y contratistas entiendan la importancia de mantener la confidencialidad de los datos personales y adopten medidas adecuadas para proteger esta confidencialidad.
9. Licitud: Asegúrate de que todos los tratamientos de datos personales se basen en una base jurídica válida, como el consentimiento informado del titular.
10. Portabilidad: Desarrolla procedimientos para permitir a los titulares de datos transferir sus datos personales a otra entidad bancaria cuando así lo soliciten.

Acciones recomendadas

- Políticas y Procedimientos: Desarrolla políticas internas y procedimientos que reflejen estos principios y asegúrate de que sean conocidos y comprendidos por todos los empleados.
- Capacitación: Realiza programas de capacitación para que todos los empleados entiendan y apliquen correctamente los principios de protección de datos.
- Auditorías y Revisiones: Asegúrate que el área de auditoría interna tenga incluido en su plan anual los temas de protección de datos en toda la entidad bancaria. Es decir que se cumplan las políticas y procedimientos de protección de datos y toma medidas correctivas cuando sea necesario.
- Comunicación y Transparencia: Mantén canales de comunicación abiertos con los titulares de los datos, proporcionando información clara y accesible sobre el tratamiento de sus datos y sus derechos. Esto lo puedes lograr implementando el aviso de privacidad en el sitio web de la entidad bancaria.
- Seguridad de la Información: Colabora con unidad responsable de definir e implementar las medidas técnicas y organizativas de Seguridad de la Información para garantizar que las mismas sean robustas y los datos personales se encuentren protegidos.

6. ¿En qué consiste el principio de transparencia? (Art. 6)

Se interpreta como la obligación de los responsables del tratamiento de datos de informar de manera clara, accesible y comprensible a los titulares de los datos sobre cómo se van a tratar sus datos personales.

Formalidades para el Tratamiento de Datos Personales:

La información se le debe brindar a los clientes de forma clara, palabras sencillas y fácil acceso, considerando lo siguiente:

1. *Identidad bancaria del responsable del Tratamiento (Entidad bancaria Bancaria)*
2. *Consentimiento para el tratamiento de los datos.*
3. *Datos recabados por la entidad bancaria*
4. *Base Legal del Tratamiento*
5. *Derechos de los Titulares de los Datos*
6. *Como se protegen los datos*
7. *Cuando y dónde comparte la información recopilada.*
8. *Duración del Tratamiento*
9. *Procedimientos para Ejercer Derechos*

Acciones Recomendadas

- *Con apoyo del área como Jurídico, Riesgo, Experiencia de Usuario y Mercadeo de cada entidad bancaria, se debe desarrollar un Aviso de Privacidad y/o Política de Privacidad de Datos, que debe estar publicado en sitio web para que los clientes tengas acceso.*
- *Se sugiere mantener un aviso de privacidad por grupo de interés (clientes, colaboradores, proveedores, directores y accionistas).*
- *En caso de actualización al Aviso de privacidad, se le debe notificar al titular de los datos por los canales oficiales definidos por cada entidad bancaria.*

7. ¿Qué significa el principio de licitud a través del consentimiento? (Art. 7)

La interpretación de este principio es que todos los clientes o titulares de los datos que entreguen información a la entidad bancaria deben dar su consentimiento previo al tratamiento de sus datos personales.

Como Oficial de Protección de Datos de la entidad bancaria, es fundamental que garantice que en todos los procesos de vinculación y cualquier otro

procedimiento que implique el tratamiento de datos personales, se obtenga la autorización previa del cliente o titular de los datos.

Para cumplir con este requisito, se recomienda implementar un formulario, sección o documento (ya sea físico o digital), donde se informe claramente al cliente sobre:

- *Los usos específicos que se le darán a sus datos.*
- *Los derechos que tiene el titular en relación con su información personal.*
- *Si los datos serán transferidos a terceros (mediante cláusulas de protección de datos).*

NOTA: *Es fundamental que este proceso se realice en coordinación con el área de Asesoría Legal de la entidad bancaria, para asegurar que se cumpla con todos los requisitos legales aplicables.*

Acciones recomendadas

- *Garantizar que el consentimiento sea otorgado de manera libre, sin presiones ni coerción por parte del banco o terceros.*
- *Procurar que el consentimiento abarque todos los posibles tratamientos que la entidad bancaria requiere realizar por el tipo de negocio. Para los casos de nuevos tratamientos, es necesario obtener el un nuevo consentimiento del cliente.*
 - *Ejemplo: si en el consentimiento otorgado no se consideró tratamientos de datos biométricos, se deberá obtener un nuevo consentimiento, antes de tratar este tipo de datos.*
- *Garantizar que el cliente tenga la capacidad legal para otorgar el consentimiento, especialmente en casos que involucren a menores de edad o personas con capacidad reducida.*

8. ¿Cuáles son los derechos ARCOP (Acceso, Rectificación, Cancelación, Oposición, Portabilidad)? (Art. 8 y 9)

La entidad bancaria deberá desarrollar y ofrecer mecanismos sencillos, accesibles y gratuitos, que permitan, el pleno y efectivo ejercicio de los derechos de protección de datos por parte de los clientes de manera oportuna y eficiente. Igualmente, deberá asegurarse de atender la solicitud efectuada en el tiempo que establece el presente Acuerdo.

Es importante mencionar que la ley se refiere a los derechos ARCO, pero debe considerar que la portabilidad es un derecho también, por lo tanto, usted podría denominar dentro de su institución de forma general Derechos ARCOP.

Adicional, se debe aclarar que el ejercicio de un derecho ARCOP no es un reclamo, pero el incumplimiento en la atención de un derecho ARCOP puede ocasionar que el cliente interponga un reclamo relacionado.

Acciones recomendadas

- *Definir dentro de la política y procedimientos el manejo de las solicitudes de atención a clientes en función de los derechos ARCOP.*
 - *Definir el lineamiento para acreditar la identidad de los titulares de los datos o de su representante legal.*
- *Habilitar mecanismos para que los titulares de los datos puedan gestionar o ejercer sus derechos ARCOP (acceso, rectificación, cancelación, oposición y portabilidad) de sus datos personales y dar seguimiento a las solicitudes presentadas. Considerando las limitaciones de cada uno de ellos.*

Ejemplos:

- *Contar con un formulario digital en página web donde el titular de los datos pueda hacer uso de este derecho de manera fácil, adicional, contar con un correo alterno al del OPD para estas comunicaciones.*
 - *Establecer un formato electrónico estructurado y comúnmente utilizado (por ejemplo, CSV) para la entrega y portabilidad de los datos solicitados.*
 - *Dar la opción para entregar los datos en papel o en formato electrónico.*
- *Establecer canales de comunicación (electrónicos y/o físicos) para recibir solicitudes y notificaciones relacionadas con los derechos ARCO. Esto se define internamente en la política y en el aviso de privacidad (de cara al cliente).*
 - *Informar a los clientes sobre sus derechos ARCO y cómo ejercerlos.*
 - *Capacitar al personal del banco sobre la importancia de la protección de datos personales, incluyendo la atención de solicitudes y reclamos relacionados con los derechos ARCO.*
 - *La entidad bancaria debe mantener registros y/o documentación de respaldo sobre las solicitudes o reclamos relacionados con los derechos*



ARCO, incluyendo las fechas de recepción y la respuesta dada a las mismas.

NOTA: *Analizar a fondo con el equipo legal de la entidad bancaria el artículo 9 del Acuerdo 01-2022 para poder aplicar las restricciones que se refieren a cada derecho específico.*

Sección 3. Tratamiento de Datos Personales

9. ¿Cuáles son las condiciones y formalidades para el tratamiento de datos personales? (Art. 10)

El Artículo 10 establece las condiciones y formalidades que deben cumplirse para el tratamiento de datos personales por parte de la entidad bancaria. Este destaca la importancia del consentimiento previo, informado e inequívoco del titular de los datos o su representante autorizado para cualquier tratamiento de datos personales, a menos que apliquen excepciones establecidas en el Acuerdo de Régimen de Protección de Datos Personales u otras leyes especiales.

Formalidades para el Tratamiento de Datos Personales:

- *Implementar procesos y procedimientos claros para obtener el consentimiento del titular de los datos o su representante autorizado antes de realizar cualquier tratamiento de datos personales y asegurar que estos sean informados y específicos.*
- *Establecer mecanismos para asegurar que el consentimiento sea efectivo, libre, informado e inequívoco, cumpliendo con los requisitos específicos del artículo.*
- *Garantizar que no se condicione la ejecución de un contrato o la prestación de un servicio al tratamiento de datos personales para finalidades que no estén relacionadas con la relación precontractual o contractual del cliente.*
- *Las condiciones para que un tratamiento de datos personales sea lícito son las siguientes:*
 1. *Interés legítimo*
 2. *Contrato*
 3. *Obligación legal*
 4. *Intereses vitales del titular de los datos*
 5. *Interés público*
 6. *Consentimiento*

- *Desarrollar mecanismos para demostrar con certeza el consentimiento otorgado o negado por el cliente y que este haya sido proporcionado en cumplimiento de los principios del régimen de protección de datos personales.*



Acciones recomendadas:

- **Proceso de obtención de consentimiento:** *Implementar un proceso claro y transparente para obtener el consentimiento del titular de los datos. Esto puede incluir:*
 - *Proporcionar información clara y detallada sobre los propósitos del tratamiento de datos.*
 - *Ofrecer opciones claras y sencillas para que el titular de los datos otorgue o rechace su consentimiento.*
 - *Utilizar medios adecuados para obtener el consentimiento, como formularios escritos o medios electrónicos que garanticen la identidad bancaria del titular de los datos.*

- **Revisión de contratos y servicios:** *Revisar y actualizar los contratos y servicios ofrecidos por la entidad bancaria para garantizar que no se condicione la ejecución de un contrato o la prestación de un servicio al tratamiento de datos personales para fines no relacionados.*
- **Documentación del consentimiento:** *Establecer un sistema para documentar y almacenar el consentimiento otorgado por el cliente, asegurando que se puedan demostrar con certeza los consentimientos obtenidos.*
- **Formación y concientización:** *Capacitar al personal sobre la importancia del consentimiento y los procedimientos para obtenerlo correctamente, asegurando que estén familiarizados con los requisitos legales y las mejores prácticas en materia de protección de datos.*
- **Revisión y actualización continua:** *Realizar revisiones periódicas de los procesos y procedimientos relacionados con el consentimiento para garantizar su eficacia y cumplimiento continuo con las regulaciones y mejores prácticas.*

Otras consideraciones

- *Para demostrar el consentimiento otorgado por el cliente, la entidad bancaria deberá obtenerlo ya sea al momento de firmar un contrato de servicios, al momento de que cambien los términos y condiciones, o se dispondrá de una campaña para obtenerlo de forma explícita y específica. Es recomendable que los contratos sean actualizados para que el otorgamiento del consentimiento reúna las características de informado, inequívoco, específico y previo.*
- *Esto podrá realizarse por medio de un formulario impreso o a través de un canal electrónico, como una campaña de correo electrónico o un mensaje en la banca en línea. Además, es importante organizar las finalidades del uso de los datos personales para que el cliente pueda aceptar o rechazar cada una de forma individual, así como permitirles elegir el canal preferido para recibir comunicaciones (teléfono, email, SMS, WhatsApp, etc.). El banco debe llevar un registro de lo anterior para demostrar con certeza que se cuenta con el consentimiento, y los clientes*

deben estar en la facultad de retirar o modificar un consentimiento en el futuro de forma fácil.

10. ¿Qué es un aviso de privacidad y qué debe contener? (Art. 11)

Un aviso de privacidad es una declaración formal que informa a los titulares de los datos sobre los aspectos clave del tratamiento de sus datos personales. Este documento debe estar disponible al momento de recopilar los datos y debe ser comprensible y accesible para todos los clientes.

Según el artículo 11, El aviso de privacidad es un documento esencial en la gestión de datos personales. Las entidades bancarias están obligadas a proporcionar este aviso a los titulares de los datos al momento de la recolección. El objetivo principal del aviso de privacidad es garantizar la transparencia en el tratamiento de los datos personales y proporcionar a los titulares información clara y accesible sobre cómo se manejarán sus datos.

¿Qué debe contener un aviso de privacidad según el Artículo 11?

El aviso de privacidad debe incluir los siguientes elementos esenciales:

- **Definiciones**

Es esencial que el aviso de privacidad comience con una sección de conceptos básicos para aclarar los términos clave utilizados a lo largo del documento, por ejemplo, "datos personales", "titular de los datos", "responsable del tratamiento", "encargado del tratamiento", entre otros, según lo establecido por la Ley 81, artículo 4.

- **Objetivo de este Aviso de Privacidad**

El aviso debe expresar claramente su objetivo, que es informar al titular de los datos personales sobre cómo sus datos serán recopilados, utilizados, almacenados y protegidos, en cumplimiento con la Ley 81, su reglamentación y el acuerdo 01-2022.

- **Información del responsable del tratamiento**

Debe incluirse la información del responsable del tratamiento de los datos, que generalmente es la entidad bancaria que recopila los datos personales. Esto incluye:

- *Nombre o razón social.*

- *Dirección física y de contacto.*
- **Oficial de Protección de Datos**
Se debe informar al titular de los datos que existe un Oficial de Protección de Datos designado en la entidad bancaria quien es responsable de garantizar el cumplimiento de la normativa de protección de datos dentro de la organización y facilitar los canales a través de los cuales puede contactarlo (teléfonos y/o correo electrónico).

NOTA: *cada entidad bancaria debe analizar su proceso de servicio al cliente para poder incluir la interacción con el oficial de protección de datos dentro de sus procedimientos.*

- **Finalidad del Tratamiento**
Se deben detallar las finalidades específicas para las cuales se utilizarán los datos personales, como la gestión de cuentas, análisis de crédito, marketing personalizado, cumplimiento de obligaciones legales, entre otros. Es importante que estas finalidades sean explícitas y que el titular esté consciente de ellas antes de proporcionar sus datos.
- **Condición de Legitimación**
Es necesario explicar la base legal que legitima el tratamiento de los datos personales, ya sea el consentimiento del titular, el cumplimiento de una obligación legal, la ejecución de un contrato, el interés legítimo del responsable, entre otras posibles bases establecidas en la Ley 81, su reglamentación y el acuerdo 01-2022.

NOTA: *recuerde que la redacción debe ser en lenguaje sencillo.*

- **Transferencia de Datos a Otros Destinatarios**
Debe informarse si los datos personales serán transferidos a terceros, incluyendo:
 - *Identificación de los destinatarios o categorías de destinatarios.*
 - *Finalidades de la transferencia.*
 - *Mecanismos de protección para dichas transferencias, especialmente si se trata de transferencias internacionales.*

- **Retención de Datos**

- **Duración del almacenamiento:** Informar sobre el tiempo durante el cual los datos personales serán conservados, basándose en requisitos legales o interés legítimo asociado al producto o servicio.
- **Criterios de eliminación:** Explicar de forma genérica los criterios utilizados para determinar cuándo los datos serán eliminados o anonimizados, de acuerdo con la normativa vigente.

- **Sus Derechos como Titular de los Datos**

Debe incluir una definición clara y concisa sobre los derechos que tiene el titular de los datos, como el derecho de acceso, rectificación, cancelación, oposición y portabilidad (derechos ARCOP), así como cualquier otro derecho que la Ley 81 reconozca.

- **Cómo Ejercer sus Derechos ARCO**

Detallar los canales disponibles para que los titulares puedan ejercer sus derechos ARCO, incluyendo:

- Sucursales
- Medios electrónicos (correo, plataformas tecnológicas, otros)
- Persona de contacto

NOTA: debe realizar un análisis a lo interno de la entidad bancaria para poder aplicar las medidas técnicas u organizativas necesarias.

- **Decisiones Automatizadas:** Indicar dentro del aviso de privacidad si el tratamiento de los datos incluye decisiones 100% automatizadas, es decir, basadas únicamente en criterios de una inteligencia artificial u otra tecnología avanzada, que puedan afectar significativamente al titular, esto debe ser claramente indicado, junto con información sobre la lógica utilizada, la importancia y las consecuencias previstas de dicho tratamiento, si aplica.
- **Actividades de Procesamiento de Datos/ finalidad del uso de los datos:** Describir de manera general las actividades de procesamiento de datos que se llevarán a cabo, cómo se gestionarán estos datos internamente y cualquier subcontratación o transferencia de datos a terceros que pueda ocurrir en el proceso de tratamiento de los datos.

- **Cookies:** *Si se utilizan cookies o tecnologías similares en las plataformas digitales de la entidad bancaria, es necesario informar sobre su uso y el propósito de las cookies.*

- **Mecanismos de Seguridad**
 - **Medidas de protección:** *Detallar las medidas de seguridad implementadas para proteger los datos personales, como encriptación de datos, firewalls, controles de acceso y auditorías de seguridad.*

 - **Compromiso con la Seguridad:** *Reafirmar el compromiso de la entidad bancaria con la protección de los datos personales, destacando las políticas y procedimientos internos destinados a prevenir accesos no autorizados, pérdidas o divulgaciones indebidas.*

- **Vigencia de este Aviso:** *Indicar desde cuándo es efectivo este aviso de privacidad y cómo se comunicarán a los titulares de los datos cualquier cambio significativo en el contenido del aviso.*

Por ejemplo: dd/mm/aaaa de la última actualización o número de la versión vigente.

- **Autoridad de Control y Regulador Superintendencia de Bancos:** *Informar a los titulares sobre su derecho a presentar quejas ante la Superintendencia de Bancos u otra autoridad competente en caso de que consideren que sus derechos han sido vulnerados. Proporcionar la información de contacto relevante.*

- **Reclamos o Consultas:** *Finalmente, el aviso debe incluir información sobre cómo los titulares pueden presentar consultas o reclamos relacionados con el tratamiento de sus datos personales, detallando los canales de contacto y el proceso a seguir para una resolución eficiente.*

Acciones recomendadas:

Para asegurar el cumplimiento efectivo del Artículo 11, las entidades bancarias deben seguir estos pasos clave:

Desarrollo

- Creación del Aviso: Desarrollar un aviso de privacidad detallado que cumpla con todos los requisitos legales y que esté adaptado a las características de cada servicio o producto bancario.
- Presentación clara: Presentar el aviso de privacidad de manera clara y comprensible, utilizando un lenguaje sencillo y evitando términos técnicos complejos.
- Visto bueno del área Legal (interna o externa): Consultar con expertos legales para asegurar que el aviso cumpla con todas las normativas y mejores prácticas en protección de datos.

Difusión

- Accesibilidad: Asegurar que el aviso de privacidad sea fácilmente accesible para los clientes a través de todos los canales electrónicos, físicos o cualquier otro que se llegue a crear en la entidad bancaria.
- Actualizaciones del Aviso de Privacidad: las entidades bancarias deben informarles a los clientes, a través de los canales oficiales de comunicación (electrónicos, físicos, otros), sobre las actualizaciones que hagan en el aviso de privacidad.

11. ¿Cómo se manejan los datos personales obtenidos de otras fuentes? (Art. 12)

El Artículo 12 del Acuerdo 01-2022 aborda el manejo de datos personales obtenidos de fuentes distintas a la institución final o las partes interesadas, es decir, datos adquiridos a través de terceros o medios públicos.

Para manejar adecuadamente estos datos, se deben seguir varios pasos y establecer políticas específicas para asegurar el cumplimiento de las normativas de protección de datos personales.

- **¿Qué se debe hacer para manejar estos datos adecuadamente?**

Establecer Parámetros y Lineamientos Generales

- *En caso de que la fuente de los datos sea un tercero, hay que asegurar que todos los datos obtenidos cumplan con las normativas de protección de datos, dicho de otra forma, el tercero que entrega la base de datos debe tener la autorización del dueño de los datos para compartirlo con la entidad bancaria. Debe asegurarse la trazabilidad basado en el origen y documentación de consentimiento.*
- *Si la información es pública, no es necesario obtener el consentimiento para tratar los datos personales del titular.*

En ambos casos se le debe informar al titular de los datos de donde se obtuvo su información personal.

Acciones recomendadas:

- *Desarrollar políticas y procedimientos claros para evaluar y verificar la legitimidad de las fuentes de datos de terceros, incluyendo directrices específicas sobre cómo registrar y manejar estos datos.*
- *Al momento del primer contacto con el cliente, informarle de donde se obtuvo su información y gestionar la autorización para tratar los datos por parte de la entidad bancaria.*
- *Evitar el uso de bases de datos proporcionada por terceros que no se pueda demostrar que cuentan con la autorización correspondiente del titular de los datos.*
- *Para datos obtenidos de fuentes públicas como redes sociales, internet, directorios y bases del gobierno (disponibles a consulta de todo ciudadano), se debe asegurar que se documente claramente el origen de estos datos en los registros de la organización.*
- *Utilizar datos provenientes de fuentes públicas sin necesidad de autorización del titular, pero asegurando que el uso de estos datos esté dentro de los límites legales y éticos de acuerdo con el servicio que brinda la entidad bancaria.*

- *Realizar auditorías periódicas para asegurar el cumplimiento de las normativas y la correcta implementación de las políticas de protección de datos.*
- *Informar de forma clara y transparente a los clientes sobre cómo se manejarán sus datos, incluyendo la obtención y uso de datos de terceros, dentro del aviso de privacidad.*

12. ¿Qué tratamientos de datos personales no requieren del consentimiento del titular? (Art. 13)

El Artículo 13 del Acuerdo 01-2022 establece los casos específicos en los que no se requiere el consentimiento del titular para tratar sus datos personales. Estos casos están diseñados para permitir que las instituciones cumplan con obligaciones legales, operativas y de seguridad sin necesidad de obtener el consentimiento previo de los titulares.

Para manejar adecuadamente los tratamientos de datos personales que no requieren el consentimiento del titular, se deben identificar claramente los escenarios permitidos por la ley y establecer políticas y procedimientos que aseguren el cumplimiento normativo.

Los escenarios que se encuentran dentro del alcance son:

- **Cumplimiento Contractual:** *cuando el tratamiento sea necesario para cumplir con la obligación pactada entre cliente y la entidad bancaria relacionado a los productos y/o servicios contratados.*
 - **Ejemplo:** *servicios brindados de tarjetas de crédito donde involucran las marcas y proveedores; provisión de datos a oficinas procesadoras de datos para la gestión de operaciones contables y administrativas.*
- **Seguridad bancaria:** *cuando por la seguridad de los clientes y colaboradores se mantienen cámaras de video vigilancia (CCTV) dentro de las instalaciones de las entidades bancarias.*
 - **Ejemplo:** *cámaras en la entrada de las sucursales, en la cajas, bóvedas y cajeros, entre otros.*

- Cumplimiento Legal o normativo: Cuando la información sea requerida por una autoridad competente de conformidad con la ley.
 - Ejemplo: atención de oficios, inspecciones judiciales, reportes regulatorios o intercambio de información para fines fiscales.
- Prevención de Delitos: Cuando sea necesario para cumplir con leyes relacionadas con la prevención de delitos como blanqueo de capitales y financiamiento del terrorismo
 - Ejemplo: envío de reporte de operaciones sospechosas (ROS) a la Unidad de Análisis Financiero (UAF).
- Análisis de Riesgo: Cuando se realiza análisis transaccionales u operativos para identificar los posibles riesgos relacionados al producto o servicio que mantiene el cliente.
 - Ejemplo: Para agencias calificadoras con fines de análisis de riesgo, análisis del perfil de riesgo del cliente, análisis del perfil de riesgo transaccional para evitar posibles fraudes financieros, entre otros.
- Entre entidades del mismo grupo económico: Cuando los datos sean utilizados o compartidos por el banco con la propietaria de acciones bancarias, subsidiarias u otra sociedad del grupo bancario para el ejercicio de las funciones propias de la entidad bancaria, siempre que no sea para fines de mercadeo.
 - Ejemplo: actualización de datos entre banco y subsidiarias, prevención de blanqueo de capitales, investigaciones internas.
- Interés legítimo: Mientras el cliente tenga un producto o servicio con la entidad bancaria y durante el periodo legal de conservación cuando haya finalizado la relación contractual, la entidad bancaria deberá tratar sus datos personales.
- Tratamientos relacionados a otra normativa:
 - Ejemplo: revisión de referencias de crédito en la APC

NOTA: es importante realizar la gestión de la autorización del titular de los datos personales para comunicaciones publicitarias sobre productos y servicios bancarios, garantizando que dicha autorización esté claramente documentada.

Otras consideraciones

- **Capacitación y Concientización:**
 - *Capacitar al personal sobre las excepciones legales y los procedimientos para el tratamiento de datos sin consentimiento.*
 - *Asegurar que todos los colaboradores comprendan y apliquen correctamente las políticas y procedimientos establecidos.*
 - *Generar una cultura de protección de datos personales dentro de toda la organización con programas de concientización.*

- **Transparencia y Comunicación:**
 - *Mantener una comunicación clara y transparente con el titular de los datos sobre las políticas de tratamiento de datos, incluyendo las excepciones que no requieren consentimiento, a través del Aviso de Privacidad de Datos.*

 - *Incluir información sobre estas excepciones en los términos y condiciones accesibles para los titulares de los datos, asegurando que estén informados y comprendan las circunstancias bajo las cuales sus datos pueden ser tratados sin su consentimiento.*

13. ¿Quiénes son los custodios de bases de datos y cuáles son sus responsabilidades? (Art.14)

El Artículo 14 del Acuerdo 01-2022 establece que los custodios de bases de datos son las entidades y/o personas responsables de la gestión y protección de los datos personales que se encuentran en sus sistemas. Estos custodios tienen un papel fundamental en la seguridad y privacidad de la información, garantizando que se cumplan las normativas de protección de datos.

Sus responsabilidades incluyen implementar medidas técnicas y organizativas adecuadas para asegurar la seguridad de los datos, permitir acceso solo a personas autorizadas y cumplir con las leyes y regulaciones vigentes, como la Ley 81 de 2019 en Panamá. Además, deben notificar a las autoridades y a los afectados en caso de incidentes de seguridad que

comprometan la información personal, protegiendo así la privacidad y los derechos de las personas de manera ética y legal.

Identificación de Custodios de Bases de Datos

Los custodios pueden ser y no se limitan a:

- **Entidades Bancarias:** *Responsables del manejo de datos de clientes.*
- **Proveedores de Servicios:** *Terceros que procesan datos en nombre de la entidad.*
- **Empleados Designados:** *Personal que gestiona las bases de datos.*

Responsabilidades de los Custodios

Como Oficial de Protección de Datos debe verificar periódicamente que los custodios de datos cumplan con las siguientes responsabilidades:

- **Seguridad de Datos:**
 - *Implementen medidas de seguridad robustas, como cifrado y acceso restringido, para proteger los datos personales.*
- **Cumplimiento Normativo:**
 - *Garanticen que el tratamiento de datos se alinee con el régimen de protección de datos personales vigente.*
- **Registro y Documentación:**
 - *Conserven registros detallados de las actividades de tratamiento, incluyendo las razones del tratamiento y los tipos de datos involucrados (aplicando el alcance definido en el artículo 15 del Acuerdo 01-2022).*
- **Notificación de Incidentes:**
 - *Establezcan un protocolo para notificar incidentes de seguridad que afecten datos personales dentro de los plazos establecidos en el régimen de protección de datos personales vigente.*

Acciones recomendadas:

- **Desarrollo de Políticas Internas:** *Crear políticas claras sobre cómo los custodios de los datos deben manejar y proteger datos personales, delimitando las responsabilidades del Oficial de Protección de datos.*

- **Auditorías Periódicas:** Realizar auditorías para evaluar la efectividad de las medidas de seguridad y el cumplimiento de las normativas.

14. ¿Cómo se debe llevar el registro de transferencias de datos personales? (Art. 15)

El Acuerdo 01-2022, artículo 15 indica el deber de las entidades bancarias de mantener un registro de transferencias de datos personales a terceros conforme a lo establecido en la Ley No. 81 en su artículo 31.

*Señala que se considerarán transferencias de datos personales a los datos transferidos a los proveedores de servicios bancarios y que cuando se utilice la figura de custodio, la entidad bancaria estará en cumplimiento del régimen de protección de datos personales al solicitar a los terceros o proveedores que certifiquen el cumplimiento a través de **esquemas contractuales**, específicamente los relacionados al registro de transferencias. El cumplimiento contractual se extiende a los proveedores de los terceros.*

Hace énfasis en:

- **Responsabilidad de las entidades bancarias:** indicando que tienen la obligación de mantener un registro que documente las transferencias de datos que hayan realizado. Esto sugiere un enfoque de transparencia y responsabilidad en el manejo de datos personales.
- **Mantenimiento actualizado del registro:** El registro debe ser actualizado regularmente para reflejar las transferencias de datos más recientes. Esto garantiza que la información sea relevante y precisa en todo momento.
- **Tratamiento histórico de los datos:** El registro debe proporcionar una visión completa del historial de transferencias de datos realizadas por la entidad bancaria. Esto implica que la información registrada debe ser detallada y precisa, lo que permite rastrear cómo se han manejado los datos a lo largo del tiempo.

Para cumplir con lo expuesto cada entidad bancaria debe mantener un registro tipo matriz para llevar el control de las transferencias de datos

personales compartidas con terceros que contenga como mínimo lo siguiente:

Secuencial	Fecha del registro	Identificación o nombre de la Base de datos (descripción funcional)	Identificación o nombre del responsable de la Base de Datos (dueño de la información interno)	Naturaleza de los datos personales contenidos
Condiciones de legitimación aplicables (lista)	Finalidades del tratamiento	Método de obtención de datos	Procedimientos de tratamiento de datos	Plazo de conservación
Destino de los datos	Personas a las que pueden ser transferidos	Medidas técnicas y organizativas de seguridad	Procedimientos para atención y respuesta del ejercicio de los derechos de los titulares de datos.	Descripción técnica de la BD (tipo de datos)
Identif. y periodo de personas que han ingresado a los datos dentro de los 15 días hábiles		Cantidad de registros		

NOTA: Ver en la sección de ANEXOS la definición de cada concepto y ejemplos para mayor detalle.

*Es importante que tomen en consideración que al final del artículo se aclara que, **las transferencias de datos del banco a un custodio de la base de datos no se considera una transferencia de datos a terceros.** En otras palabras, para este escenario, aunque los datos están siendo movidos de una parte (entidad bancaria) a otra (al custodio de la base de datos), esta acción no se considera una transferencia a terceros según los términos de este acuerdo en particular, por lo tanto, no será necesario llevar estas transferencias en el registro.*

*Para mayor claridad detallamos la diferencia entre un **custodio de la base de datos, un proveedor de servicio y un tercero:***

- **Custodio de la base de datos:** Persona natural o jurídica que, en nombre de la entidad bancaria, custodia la base de datos y los datos personales en ella contenidos (encargado del tratamiento de datos).
 - **Funciones:**
 - Realizar el tratamiento de datos según las instrucciones del responsable.
 - Garantizar la seguridad y confidencialidad de los datos.
 - Mantener registros detallados de las actividades de tratamiento.

- **Proveedor de servicios bancarios:** *Persona natural o jurídica, distinta del custodio de la base de datos, contratada por el banco para desarrollar y llevar a cabo actividades, funciones o procesos vinculados con el negocio de banca y que está involucrada en el tratamiento de datos personales.*
 - **Relación con otros conceptos:**
 - **Encargado del tratamiento:** *A menudo, un proveedor de servicios actúa como encargado del tratamiento cuando procesa datos por cuenta del responsable.*
 - **Tercero:** *También puede ser considerado un tercero si simplemente recibe datos para prestar un servicio específico.*
 - **Responsabilidad:** *La responsabilidad de un proveedor de servicios depende de su papel específico en el tratamiento de datos.*

- **Tercero:** *cualquier entidad que recibe datos personales del responsable del tratamiento, pero que no actúa como encargado del tratamiento.*
 - **Tipos de terceros:**
 - **Destinatarios:** *Aquellos a quienes se comunican los datos de forma regular.*
 - **Encargados del tratamiento:** *Aquellos que procesan los datos por cuenta del responsable (custodio de la base de datos).*
 - **Otros:** *Cualquier otra entidad que reciba datos, como autoridades gubernamentales.*
 - **Responsabilidad:** *La responsabilidad de un tercero varía según su papel. Los destinatarios, por ejemplo, deben garantizar la confidencialidad de los datos recibidos.*

TABLA RESUMEN

Concepto	Definición	Funciones principales	Responsabilidad
Custodio de datos	<i>Procesa datos por cuenta de la entidad bancaria</i>	<i>Seguir instrucciones, garantizar seguridad</i>	<i>Obligaciones específicas bajo el régimen de Protección de datos Personales</i>
Tercero	<i>Recibe datos de la entidad bancaria para objetivo específico</i>	<i>Varía según el tipo de tercero</i>	<i>Depende del rol específico</i>

Proveedor de servicios	<i>Presta servicios y puede acceder a datos de la entidad bancaria</i>	<i>Prestar servicios, procesar datos (si es encargado/ custodio)</i>	<i>Definido contractualmente y acuerdo de protección de datos personales</i>
-------------------------------	--	--	--

Acciones recomendadas:

- *Definir un proceso, roles y responsabilidades para controlar las solicitudes de reportes, query o alguna base de datos que contenga datos personales de los clientes, colaboradores, directores o proveedores, dentro del cual se pueda evaluar la proporcional de la información solicitada y las medidas técnicas y organizativas necesarias para cumplir con el régimen de protección de datos personales vigente.*
- *Centralizar y mantener actualizado los registros de las transferencias de datos a terceros garantizando que la matriz contenga como mínimo los datos indicados en los párrafos anteriores.*
- *Realizar un inventario de las bases de datos (activos de información) que contengan datos personales en la organización en los distintos sistemas y formas posibles. Este inventario puede ser llevado en Excel o en una aplicación similar. Estas bases de datos en las que se haya identificado la realización de las transferencias se registrarán en la matriz junto con todos los detalles enunciados anteriormente.*
- *Identificar los tratamientos de datos personales que se realicen sobre estas bases de datos y en cuál de estos tratamientos se ejecuta alguna transferencia de datos personales a un tercero.*
- *Para los proveedores que sean custodios, se deberá de agregar en el contrato o a través de un Acuerdo de Protección de Datos Personales, que dentro de las responsabilidades como custodio debe llevar su registro de transferencias en el caso que aplique.*
- *El área de protección de datos deberá estar informado de la puesta en marcha de los nuevos proyectos y servicios para identificar las medidas técnicas y organizativas que se deban aplicar con el fin de que se mantenga actualizado el registro de transferencias.*

- *Cuando se lleve a cabo transferencias periódicas, el área responsable llevará el registro de la actividad.*

15. ¿Qué procedimientos deben seguirse para la conservación de datos personales? (Art. 16)

*Los datos personales en el ámbito bancario deben ser gestionados con un enfoque que garantice su **confidencialidad, integridad y disponibilidad**. Esto implica que las entidades bancarias deben utilizar bases de datos seguras que protejan la información sensible, asegurando que solo personas autorizadas tengan acceso a ella. Además, los datos deben conservarse durante el tiempo estipulado en los acuerdos bancarios o en leyes específicas, lo que obliga a los bancos a cumplir con regulaciones sobre la retención de datos.*

*Una vez que el período legal de conservación ha expirado, **las entidades bancarias deben implementar medidas técnicas y organizativas razonables de control para garantizar no transferir ni comunicar datos de clientes después del período adicional de siete años, a menos que el cliente haya dado su consentimiento explícito. Esto debe estar debidamente documentado dentro de los protocolos de protección de datos.***

Finalmente, la obligación de confidencialidad persiste incluso después de que la relación entre el banco y el titular de los datos haya terminado. Esto significa que los bancos deben seguir protegiendo la información almacenada, a menos que existan excepciones legales claramente definidas que permitan la divulgación. Así, se establece un marco robusto para la protección de datos personales en el sector bancario, asegurando que la privacidad de los clientes sea una prioridad constante.

Acciones recomendadas:

- *Aplicar las medidas técnicas y organizativas que permitan el aseguramiento de los datos personales una vez terminado el periodo legal de conservación, de forma que solo estén disponible para las entidades competentes.*

Ejemplos:

- Entre las medidas organizativas, que pueden estar aplicadas para preservar la seguridad de los datos personales, sin limitarlas, tenemos:
 1. Políticas de seguridad de la información, protección de datos, ciberseguridad, respaldo de la información, entre otras.
 2. Capacitación al personal en cuanto al manejo seguro de la información y normativa de protección de datos.
 3. Firmas de acuerdos de confidencialidad con los colaboradores.
 4. Definir mecanismos de bloqueo de datos o segmentación de clientes

- Entre las medidas técnicas, sin limitarlas, están las siguientes:
 1. Herramientas de Firewalls, DLP.
 2. Gestión de acceso a los sistemas.
 3. Software Antivirus, EDR, XDR, etc.
 4. Herramientas de monitoreo: SIEM, SOC.
 5. Segmentación de redes.

NOTA: Los mecanismos variaran dependiendo del caso y los medios donde se encuentren almacenados, la idea es impedir su tratamiento incluyendo su visualización.

- Llevar un registro de plazos de conservación de datos personales (físico y digital) según los acuerdos bancarios y leyes aplicables, por tipo de documento.
- Para el registro de bases de datos transferidas a terceros, establecer los plazos de conservación que aplique para cada caso y aplicar el proceso correspondiente de eliminación.
- Levantar protocolos de destrucción, borrado y bloqueo de datos personales cuando no se mantenga o se extinga la base legitimadora para su conservación o transferencia.

16. ¿Cuándo y cómo realizar una evaluación de impacto en el tratamiento de datos personales? (Decreto 285, art. 4, numeral 9, art. 33, numeral 6 y art. 41)

El Decreto 285, que reglamenta la Ley 81 de protección de datos personales en su artículo 41 busca que las organizaciones piensen con cuidado en los riesgos para la información personal cuando implementen nuevos procesos o usen tecnologías novedosas, y que tomen medidas para proteger esa información. La Autoridad de Control y/o el regulador bancario están ahí para asegurar de que esto se haga correctamente dentro de las entidades bancarias e incluso solicitar que sean publicado dichos informes.

Una evaluación de impacto en protección de datos personales (EIPD) es un análisis previo que identifica y mide los riesgos potenciales que un tratamiento de datos personales podría generar para los derechos y libertades de los interesados. Este proceso permite tomar medidas para proteger la privacidad de las personas antes de iniciar el tratamiento.

De manera general, la evaluación de impacto en protección de datos personales (EIPD) se debe realizar, sin limitar el alcance de cada entidad bancaria, en los siguientes casos:

- Cuando el tratamiento de datos personales pueda implicar un alto riesgo para los derechos y libertades de las personas. Esto incluye tratamientos que utilizan nuevas tecnologías o que, por su naturaleza, alcance, contexto o fines, puedan generar riesgos significativos.*
- Si el tratamiento implica el uso de nuevas tecnologías que pueden afectar la privacidad de los datos personales.*
- Si se realizan cambios significativos en el tratamiento de datos que puedan aumentar los riesgos para los derechos y libertades de los interesados.*

*A continuación, tabla con ejemplos de **cuando** aplicar la evaluación de impacto:*

Criterios para EIPD	Ejemplo
Procesos nuevos o mejoras en procesos existentes que tienen dentro de su alcance recopilar o procesar información personal.	<ul style="list-style-type: none">• Creación de un nuevo flujo de originación de crédito o la mejora a un proceso existente de canje de puntos.
La información sobre individuos se compartirá con personas u organizaciones externas a la entidad.	<ul style="list-style-type: none">• Generación de reportes que se compartirán a terceros o proveedores.

<p>Cambio de uso de los datos personales existentes, con respecto al propósito inicial del tratamiento o migración de plataformas tecnológicas que involucren datos personales.</p>	<ul style="list-style-type: none"> • Utilizar los datos recabados durante la originación de préstamos de autos para otros procesos definidos por el grupo o Casa Matriz. • Migración de servidores que contienen información personal de los clientes.
<p>El uso de nuevas tecnologías o mejoras en las herramientas existentes que recopilan o utilizan datos de carácter personal.</p>	<ul style="list-style-type: none"> • Upgrade o actualizaciones de las herramientas tecnológicas existentes que implique tratar datos personales de los clientes. • Tecnologías nuevas como las relacionadas a datos biométricos, formularios digitales, RPA, otros.
<p>Los datos personales existentes se utilizarán para tomar decisiones como parte de un proceso automatizado o perfilamiento.</p>	<ul style="list-style-type: none"> • Creación de procesos automatizados para mejorar procesos existentes • Implementación de un nuevo motor de decisiones para aprobación de préstamos o mejoras a la herramienta actual.
<p>El cliente podría considerar cualquier aspecto del proyecto como intrusivo o que los datos involucrados son privados.</p>	<ul style="list-style-type: none"> • Proyectos o iniciativas de cara al cliente que impliquen el uso de datos personales
<p>Uso a gran escala de datos personales o sensibles.</p>	<ul style="list-style-type: none"> • Extracción masiva de información personal para realizar análisis de cartera de cliente.
<p>Cambio de ubicación geográfica de los datos.</p>	<ul style="list-style-type: none"> • Migración de información personal de un sitio de contingencia a otro.

*Sin limitarse a la necesidad de cada entidad, a continuación, compartimos tabla de referencia con aspectos a considerar cuando **documenta** una evaluación de impacto en protección de datos personales (EIPD):*

Aspecto Evaluado	Descripción	Riesgos Identificados	Medidas de Mitigación	Responsable	Plazo
Tipo de Datos	Datos personales sensibles (ej. salud, religión)	Riesgo de divulgación no autorizada	Encriptación de datos, acceso restringido	Equipo de TI	1 mes
Finalidad del Tratamiento	Marketing personalizado	Riesgo de uso indebido de datos	Consentimiento explícito, auditorías periódicas	Departamento de Marketing	2 semanas
Tecnología Utilizada	Sistemas de inteligencia artificial	Riesgo de decisiones automatizadas injustas	Evaluación ética, supervisión humana	Equipo de IA	3 meses
Transferencia de Datos	Transferencia a terceros países	Riesgo de incumplimiento de normativas	Acuerdos de protección de datos, evaluaciones de impacto	Departamento Legal	1 mes
Acceso a Datos	Acceso por empleados	Riesgo de acceso no autorizado	Políticas de acceso, formación en protección de datos	Desarrollo Humano	3 semanas

Sección 4. Gestión de los Datos Personales

17. ¿Cómo debe ser el sistema de control interno para la gestión de datos personales? (Art. 17)

Para dar respuesta a esta pregunta tome en consideración lo establecido en el Acuerdo 05-2011 de la Superintendencia de Bancos de Panamá (SBP), que hace referencia a los controles internos que deben establecer las entidades bancarias a través de Gobierno Corporativo, esto incluye el conjunto de políticas, principios, normas, procedimientos y mecanismos de prevención, verificación y evaluación establecidos por la Junta Directiva y la Alta Gerencia.

Es fundamental ejecutar los principios mínimos del Sistema de Control Interno, tales como el ambiente de control, evaluación del riesgo, actividades de control, información y comunicación, sistemas informáticos, monitoreo y evaluaciones independientes, según lo establece el Acuerdo 05-2011, artículo 3. El cumplimiento de estos principios debe considerarlo cuando

formalice la política de protección de datos personales (PDP), manuales, fichas técnicas o protocolos relacionados.

Acciones recomendadas:

- *Establecer políticas claras y procedimientos detallados para el manejo de datos personales, asegurando que todos los colaboradores comprendan sus responsabilidades.*
- *Realizar evaluaciones periódicas de riesgos para identificar y mitigar posibles amenazas a la seguridad de los datos.*
- *Implementar medidas técnicas y organizativas, como la encriptación de datos, control de acceso y gestión de identidades.*
- *Capacitar regularmente al personal sobre las mejores prácticas de seguridad y privacidad de datos.*
- *Monitorear continuamente el sistema y realizar auditorías internas para asegurar el cumplimiento de las políticas y procedimientos establecidos.*
- *Adoptar un enfoque de mejora continua, revisando y actualizando las políticas y procedimientos según sea necesario para adaptarse a nuevas amenazas y cambios regulatorios.*

18. ¿Cuáles son las responsabilidades de la junta directiva en la protección de datos personales? (Art. 18)

La Junta Directiva es responsable de garantizar una estructura organizativa adecuada, aprobar recursos, políticas y procedimientos y fomentar una cultura de protección de datos.

Es importante tener en cuenta lo establecido en el Art. 13 del Acuerdo 05-2011 y el Art. 18 del Acuerdo 01-2022, que detallan las responsabilidades de la junta directiva. Estas responsabilidades deben estar claramente plasmadas en la política de protección de datos personales.

La Junta Directiva debe ser informada sobre las medidas técnicas, organizativas y de control implementadas para el cumplimiento de la normativa, a través de los canales establecidos por la entidad bancaria, ya sea mediante comités o capacitaciones en temas relacionados con la protección de datos personales.

Es necesario ajustar la documentación de gobierno corporativo para establecer el rol de la Junta Directiva en alineación con la protección de datos personales.

19. ¿Qué implica la certificación de cumplimiento de la junta directiva? (Art. 19)

El acuerdo 01-2022, en el artículo 19, establece que las entidades bancarias deben presentar anualmente a la Superintendencia una certificación firmada por el presidente y el secretario de la Junta Directiva, asegurando que conocen los estándares de protección de datos, que tienen políticas y procedimientos para gestionar la protección de datos y que están informados sobre la efectividad de las medidas de protección de datos.

Para las sucursales de bancos extranjeros, pueden presentar una certificación de su casa matriz demostrando cumplimiento equivalente.

Las certificaciones deben ser entregadas dentro de los 60 días posteriores al cierre fiscal y pueden ser apostillados/notariadas o realizadas con firma electrónica calificada.

Acciones recomendadas:

- *Lograr implementar un plan de concienciación y formación continua para los colaboradores y miembros de la Junta Directiva sobre los estándares y regulaciones de protección de datos vigentes, así como sobre las implicaciones de no cumplir con estas normativas.*
- *El Oficial de Protección de datos Personales debe proporcionar informes periódicos a la Junta Directiva sobre la efectividad de las medidas de protección de datos implementadas, incluyendo incidentes de seguridad, acciones correctivas tomadas y actualizaciones sobre cambios en las regulaciones.*
- *A través del Oficial de Protección de datos, dar seguimiento a la preparación y presentación de la certificación anual de cumplimiento, firmada por el presidente y el secretario de la junta directiva, dentro del plazo establecido y con las garantías de autenticidad requeridas.*

- *Por medio de la Junta Directiva o alta dirección, aprobar los cambios en las políticas y procedimientos de protección de datos para asegurar que sigan siendo efectivos y estén alineados con los requisitos normativos cambiantes.*

20. ¿Qué funciones tiene la unidad de administración de riesgo en relación con la protección de datos personales? (Art. 20)

El Acuerdo 01-2022, artículo 20 establece que la Unidad de Administración de Riesgo de una entidad bancaria tiene la responsabilidad de identificar, evaluar y controlar los riesgos asociados con la protección de datos personales. Esto implica que la unidad debe considerar los posibles peligros o amenazas que puedan surgir en relación con la seguridad y confidencialidad de los datos personales de los clientes, así como las medidas necesarias para mitigar estos riesgos.

En resumen, la interpretación del artículo indica que la Unidad de Administración de Riesgo debe integrar la protección de datos personales dentro de sus procesos de gestión de riesgos, asegurando que se tomen las medidas adecuadas para proteger la información confidencial y cumplir con las regulaciones pertinentes.

Acciones recomendadas:

- *Realizar una evaluación exhaustiva y continua para identificar los riesgos potenciales asociados con la protección de datos personales en todas las operaciones y procesos del banco, documentando las posibles amenazas, vulnerabilidades y consecuencias potenciales para la seguridad de la información. Todo esto a través de la Unidad de Administración de Riesgo de la entidad bancaria.*
- *Una vez identificados los riesgos, evaluarlos en términos de su probabilidad de ocurrencia y el impacto que tendrían en la confidencialidad y seguridad de los datos personales.*
- *Desarrollar e implementar medidas y controles adecuados para mitigar los riesgos identificados, como la encriptación de datos, el acceso restringido a la información, la capacitación del personal en seguridad de la información, entre otros.*

- *Monitorear continuamente la efectividad de los controles implementados y revisar periódicamente la efectividad de las medidas de protección de datos, realizando ajustes según sea necesario, a través de la Unidad de Administración de Riesgo.*
- *Fomentar la colaboración entre la Unidad de Administración de Riesgo y otras áreas relevantes, como el área de tecnología de la información, el área legal y el área de cumplimiento, para abordar de manera integral los riesgos de protección de datos.*
- *Mantenerse al tanto de las últimas tendencias y desarrollos en materia de protección de datos y gestión de riesgos, y ajustar los procesos y controles en consecuencia para mantener la efectividad y relevancia.*
 - **Ejemplo/caso de uso:** *La Unidad de Administración de Riesgo identifica el riesgo de brechas de seguridad en la base de datos de la entidad bancaria debido a un acceso no autorizado al sistema. Para mitigar este riesgo, implementa medidas de seguridad adicionales, como la autenticación de dos factores y el monitoreo continuo de la actividad del sistema. Esto reduce la probabilidad de que se produzcan violaciones de datos y protege la información confidencial de los clientes.*

NOTA: *el Oficial de Protección de Datos debe proporcionar formación adecuada y continua al personal de la Unidad de Administración de Riesgo sobre las regulaciones de protección de datos y su relación con la gestión de riesgos y seguridad de la información.*

21. ¿Cómo se realiza la auditoría interna y el seguimiento del sistema de control interno? (Art. 21)

El Artículo 21 establece que las entidades deben implementar mecanismos de auditoría interna y seguimiento continuo del sistema de control interno para garantizar el cumplimiento de las normas de protección de datos. Estas auditorías son esenciales para identificar riesgos, evaluar la eficacia de las medidas de seguridad y asegurar que las operaciones de tratamiento de datos cumplan con la normativa vigente.

Aspectos Clave de las Auditorías Internas

Las auditorías internas deben enfocarse en:

- **Cumplimiento Normativo:** Verificar que las políticas y procedimientos estén alineados con la Ley 81, el Decreto 285 que la reglamenta y el Acuerdo 01-2022.
- **Identificación de Riesgos:** Detectar debilidades en la gestión y seguridad de los datos personales.
- **Propuestas de Mejora:** Ofrecer recomendaciones que fortalezcan el sistema de control interno.
 - **Ejemplo/ Caso de Uso:** como parte de un proceso de auditoría interna, se le podrán solicitar al Oficial de Protección de Datos los siguientes documentos:
 - Políticas de Protección de datos actualizada
 - Aviso de Privacidad publicado
 - Consentimientos
 - Manual de Protección de datos
 - Presentaciones a Junta directiva o Comité con sus respectivas minutas.
 - Registro de Derechos ARCOP y evidencias
 - Manejo de Incidentes de Seguridad de la Información
 - Registro de Transferencia a Terceros
 - Descriptor de Puestos del Oficial de Protección de Datos
 - Inventario de Canales de captación de datos de clientes y/o colaboradores

Lineamientos para el Seguimiento del Sistema de Control Interno

El seguimiento debe garantizar que:

- **Existan indicadores de desempeño:** Se monitoreen aspectos como incidentes de seguridad, cumplimiento en solicitudes de titulares (derechos ARCOP) y eficacia de las medidas implementadas.
- **Se realicen revisiones periódicas:** Se establezca un calendario para evaluar áreas críticas.
- **Se documenten resultados:** Mantener registros de los hallazgos y las acciones correctivas implementadas.

Acciones recomendadas:

Para llevar a cabo auditorías internas y seguimiento eficaz, se sugiere:

- **Alinear al equipo de auditoría interna:**
 - Realizar sesiones de trabajo para homologar los controles requeridos para el cumplimiento del régimen de protección de datos personales.
- **Adaptar el enfoque a la institución:**
 - Considerar el tamaño y la complejidad de las operaciones de la entidad.
 - Priorizar áreas de mayor riesgo.
- **Capacitar al personal:**
 - Proveer formación básica sobre protección de datos a los responsables de auditorías y seguimiento.
- **Establecer un proceso flexible:**
 - Diseñar procedimientos que permitan ajustes según cambios normativos o tecnológicos.

22. ¿Qué debe considerar la entidad bancaria cuando designa al Oficial de Protección de Datos? (Art. 22)

El Artículo 22 del Acuerdo 01-2022 establece que cada entidad bancaria debe designar obligatoriamente un Oficial de Protección de Datos (OPD), considerando la estructura organizacional y asegurando la independencia necesaria para el desarrollo de sus funciones. El OPD es clave para supervisar el cumplimiento de la normativa y proteger los derechos de los titulares de datos.

Facultades del OPD

- **Independencia y Autoridad**

El OPD debe desempeñar sus funciones con total independencia dentro de la organización, reportando directamente a la Gerencia Superior o Alta Dirección. Esto asegura que sus decisiones sean tomadas sin interferencias y con la autoridad necesaria. Además, debe contar con suficiente jerarquía dentro de la estructura organizativa para garantizar su eficacia y autonomía.

- *Gestión de la confidencialidad*
El OPD tiene la obligación de mantener la confidencialidad de la información obtenida durante el ejercicio de sus funciones. Esta responsabilidad es clave para preservar la integridad y la confianza en el tratamiento de los datos personales.
- *Supervisión del cumplimiento normativo*
El OPD debe velar por el cumplimiento de las normativas relacionadas con la protección de datos personales, asegurándose de que las políticas internas sean actualizadas conforme a los requisitos del Régimen de Protección de Datos Personales y del presente Acuerdo.
- *Informe a la junta directiva o comité designado*
Deberá informar regularmente a la Junta Directiva o al Comité designado sobre la eficacia de los programas y medidas implementadas en cuanto a protección de datos. Esto incluye el cumplimiento de las obligaciones regulatorias y la evaluación continua de los controles aplicados.
- *Recursos y apoyo organizativo*
La entidad bancaria deberá proporcionarle al OPD los recursos necesarios para que pueda desempeñar su labor adecuadamente, garantizando que esté involucrado en todos los asuntos relacionados con la protección de datos personales.
- *Experiencia y capacitación profesional*
El OPD debe contar con experiencia profesional en áreas relacionadas con la banca o el sector financiero y contar con capacitaciones en materia de protección de datos. Su nombramiento o reemplazo deberá ser notificado previamente a la Superintendencia de Bancos.
- *Procurar la independencia funcional*
A fin de asegurar la plena independencia del OPD, el banco deberá estructurar su organización de manera que se evidencie la jerarquía y autonomía de este cargo dentro de la entidad.

Para elegir al OPD, la organización debe considerar a la persona que reúna el perfil que más se asemeje a lo requerido por el Acuerdo 001-2022 y el Decreto 285 que reglamenta la Ley 81 de Protección de datos Personales. Más allá del conocimiento sobre asuntos relacionados con los datos

*personales, aspectos legales y tecnológicos, **la autonomía y acceso a la alta gerencia** son un factor de gran relevancia para asegurar el éxito de un programa de protección de datos personales.*

*Además de las áreas excluidas (auditoría, riesgo, cumplimiento), debe evitarse otras áreas, en la medida de lo posible, donde puedan existir **conflictos de interés** que afecten el ejercicio de los derechos de los titulares de los datos (clientes, colaboradores, etc.).*

*Es importante la asignación de **recursos adecuados** (personal suficiente e idóneo, sistemas de información y procesos adecuados) para el cumplimiento del régimen de protección de datos personales.*

No debemos perder de vista que el responsable del tratamiento de los datos en todo momento es la entidad bancaria, no el OPD. Es decir, el apoyo de los más altos niveles directivos y gerenciales es fundamental para el cumplimiento, ya que de ellos deriva la autoridad y los recursos para implementar los cambios en los procedimientos requeridos que lleven a una cultura de protección de datos personales en el banco.

Acciones recomendadas

- *Incluir en el descriptor de puestos o en el alcance de las funciones del Oficial de Protección de Datos de Desarrollo Humano el listado de las funciones tal como aparece en el Acuerdo 01-2022, artículo 23.*
- *Esto debe concordar con lo que defina la entidad bancaria dentro de los roles y responsabilidades de la Política de Protección de datos Personales (interna).*
- *Notificar a través de una nota formal a la Superintendencia de Banco de Panamá la designación o reemplazo del Oficial de Protección de datos.*
- *Circular SBP-DR-0071-2022 es donde se recibe la instrucción de reportar en el AT05 el nombre del Oficial de Protección de datos designado por la entidad bancaria. La circular no indica que debe reportarse los datos del encargado temporal o personal interino que ocupe el rol del OPD durante vacaciones o ausencias temporales a la SBP.*

- *En base a lo que indica el Acuerdo 001-2022, el OPD debe reportar a la alta gerencia o gerencia general.*

NOTA: *El cómo se desarrollan estas funciones debe quedar documentado en los protocolos generales/ ficha técnica de la gestión de Protección de datos personales.*

23. ¿Cuáles son las funciones específicas del oficial de protección de datos (OPD)? (Art. 23)

Las funciones específicas del Oficial de Protección de Datos (OPD) dentro de las entidades bancarias se encuentran establecidas en el Acuerdo 01-2022, artículo 23 y en el Decreto Ejecutivo No. 285 de 2021, artículo 44.

A continuación, las funciones establecidas según normativa para el OPD:

- *Registro de sucesos de Protección de Datos*

Documentar todos los sucesos que comprometan la seguridad de los datos personales; mantener este registro ayuda a analizar patrones y prevenir futuros incidentes.

Entendiendo que un suceso puede referirse a eventos, incidentes, quejas o reclamos donde existe la posibilidad de una afectación en el tratamiento de datos personales.

- *Reporte de deficiencias*

Identificar y reportar cualquier deficiencia en las medidas técnicas y organizativas de protección de datos implementadas. Esto asegura que se tomen medidas correctivas oportunas para fortalecer la seguridad de los datos.

- *Incidentes de seguridad de información es cualquier evento que compromete la **confidencialidad, integridad o disponibilidad** de la información dentro de un sistema o red.*

- Por ejemplo: esto puede incluir accesos no autorizados, pérdida de datos, ataques de malware, ransomware, entre otros.

- *Deficiencias es una falla o desperfecto a nivel de procesos o sistemas.*

- Por ejemplo: en el contexto de la seguridad de datos, una deficiencia podría referirse a una carencia o insuficiencia en las medidas de seguridad, como configuraciones incorrectas, falta

de actualizaciones o errores humanos que pueden dejar vulnerables los sistemas y datos.

- *Coordinación con el Área de Seguridad de la Información*

Colaborar estrechamente con el equipo de seguridad de la información para asegurar una protección integral. Esta coordinación alinea las políticas de protección de datos con las estrategias de seguridad del banco.

- *Proporcionar sugerencias para medidas correctivas*

Recomendar acciones específicas para corregir fallas en la protección de datos. Esto contribuye a la mejora continua de las prácticas de protección de datos.

- *Comunicación con Áreas clave de la entidad bancaria*

Establecer canales de comunicación efectivos con áreas como auditoría interna, riesgos y cumplimiento. Esto asegura una colaboración efectiva en temas relacionados con la protección de datos.

- *Enlace con la Superintendencia de Bancos*

Actuar como punto de contacto entre el banco y la Superintendencia de Bancos, facilitando la comunicación y el cumplimiento de las regulaciones de protección de datos.

- *Capacitación en Protección de Datos*

Planificar y coordinar programas de capacitación en protección de datos para el personal del banco. Esto asegura que todos los colaboradores comprendan sus responsabilidades y las mejores prácticas en protección de datos.

- *Servir de enlace con los Titulares de los Datos*

Atender las consultas relacionadas a las solicitudes presentadas por los titulares de los datos a la entidad bancaria, garantizando que sus derechos sean respetados y sus dudas sean resueltas.

Acciones recomendadas:

- *Comprender la normativa vigente, esto implica que el OPD debe trabajar muy de cerca con el área Jurídica de la entidad bancaria.*

- *Analizar los procesos de negocio de la entidad bancaria e identificar los puntos de mejora necesarios para cumplir con los controles que piden la normativa vigente.*
- *Establecer formalmente los procesos y procedimientos claros donde se incluya la participación del OPD y las medidas técnicas y organizativas con el fin de cumplir de manera efectiva con el régimen de protección de protección de datos.*
- *Aplicar evaluaciones de impacto en el tratamiento de datos personales en los diferentes procesos de la entidad bancaria cuando sea requerido.*
- *Contar con evidencias de las interacciones y acuerdos llegados con las diferentes áreas de la entidad como minutas, correos, presentaciones grabaciones, entre otros.*
- *Llevar una bitácora de los sucesos, incidentes o deficiencias que surjan como parte de la gestión del día a día; esta bitácora puede incluir fecha, # de control, descripción, análisis o comentarios del OPD, resolución final, entre otros.*
- *Coordinar un plan anual de capacitación en materia de protección de datos para todo el personal de la entidad bancaria en colaboración con el área de Desarrollo Humano.*
- *Informar a la gerencia general o alta gerencia, así como a las áreas de control (Riesgo y Auditoría Interna) cuando se den los incidentes, las deficiencias o sucesos que impacten en el tratamiento de datos personales. Esto debe quedar establecido en las políticas y ficha técnica de Protección de datos.*
- *Presentar un informe sobre la eficacia de los programas, medidas y controles relacionados con la protección de datos personales, en las reuniones periódicas de la junta directiva. Este informe también incluirá el estado de cumplimiento de las obligaciones regulatorias en esta materia. La periodicidad de las reuniones se establecerá en función de las necesidades de cada entidad y se documentará en la ficha técnica de Protección de datos.*

Sección 5. Tratamiento y Transferencia de los Datos Personales

24. ¿Qué medidas técnicas y organizativas deben adoptarse para el tratamiento de datos personales? (Art. 24)

Cada entidad bancaria tiene la obligación de establecer y documentar procedimientos y procesos para el tratamiento de datos personales, según se establece en el artículo 24 del acuerdo 01-2022.

Es importante impulsar la aprobación de políticas generales y específicas sobre Protección de Datos Personales para cumplimiento de la Ley 81, su reglamentación y el acuerdo 01-2022. Se requiere que estos procedimientos y procesos se basen en las normas sobre protección de datos personales y en las políticas de tratamiento de protección de datos adoptadas por la entidad y aprobadas por la Junta Directiva.

Para estas definiciones el Oficial de Protección de Datos (ODP) debe trabajar en conjunto con el área de Asesoría Legal/ Jurídica, Seguridad de la Información, procesos y otras áreas que guarden relación con la protección de los datos personales de los clientes, colaboradores y proveedores, con el fin de lograr la sinergia entre todas.

Acciones recomendadas

- **Definir procedimientos a criterio de cada entidad bancaria que abarquen:**
 - **La inclusión:** establecer cómo se recolectan los datos y qué información se debe obtener del titular de los datos.
 - **La conservación y almacenamiento:** definir medidas de seguridad y plazos de retención.
 - **La modificación:** establecer quién puede realizar cambios en los datos y cómo se documentan.
 - **La supresión:** definir los criterios y procedimientos para eliminar los datos de manera segura.
 - **La transferencia:** establecer requisitos y procedimientos para transferir datos a terceros.

- **Adoptar políticas de tratamiento de protección de datos personales:**
 - *Desarrollar políticas internas alineadas con las normativas legales y las mejores prácticas de protección de datos.*
 - *Asegurar que estas políticas sean aprobadas por la junta directiva y comunicadas a todo el personal.*

- **Documentar y comunicar los procedimientos y políticas:**
 - *Documentar todos los procedimientos y políticas en un manual de protección de datos personales.*
 - *Capacitar al personal sobre estos procedimientos y políticas para garantizar su comprensión y cumplimiento, cuando sea necesario.*

- **Implementar controles y auditorías regulares:**
 - *Establecer controles internos para monitorear el cumplimiento de los procedimientos y políticas.*
 - *Realizar auditorías periódicas para garantizar el cumplimiento continuo y la efectividad de los procesos de tratamiento de datos personales.*

25. ¿Cómo se garantiza la seguridad en el tratamiento de datos personales? (Art. 25)

Este artículo establece la obligación para las entidades bancarias de asegurarse de que el tratamiento y la transferencia de datos personales se realicen de manera segura. Esto implica sin limitar las disposiciones establecidas en el Acuerdo para la Gestión del Riesgo de la Tecnología de la Información¹ y el Acuerdo sobre Banca Electrónica emitidos por la Superintendencia de Bancos².

Con el fin de garantizar la seguridad en el tratamiento y transferencia de datos se deben implementar medidas de seguridad para proteger la

¹ ACUERDO No. 003-2012 (de 22 de mayo de 2012) “Por el cual se establecen lineamientos para la gestión del riesgo de la tecnología de la información”

² ACUERDO No. 006-2011 (de 6 de diciembre de 2011) “Por medio del cual se establecen lineamientos sobre banca electrónica y la gestión de riesgos relacionados”

confidencialidad, integridad y disponibilidad de los datos por parte del equipo de Seguridad de la información o área designada.

Es importante que la comunicación sea fluida entre Seguridad de la Información y el OPD para que exista coherencia entre las estrategias de ambas áreas y se pueda coordinar con efectividad el programa de protección de datos de la entidad bancaria.

Acciones recomendadas

A nivel de Seguridad de la información, les dejamos algunas medidas sugeridas, pero sin limitar las que a bien adicionales quieran implementar.

1. Implementar medidas de seguridad adecuadas:

- Utilizar tecnologías de cifrado para proteger la información sensible durante su almacenamiento y transmisión.*
- Establecer controles de acceso para limitar el acceso a los datos personales solo a personal autorizado.*
- Implementar sistemas de monitoreo y detección de intrusiones para identificar y responder a posibles amenazas de seguridad.*

2. Aplicar las disposiciones de los acuerdos pertinentes:

- Revisar y comprender las disposiciones del Acuerdo para la Gestión del Riesgo de la Tecnología de la Información y el Acuerdo sobre Banca Electrónica emitidos por la Superintendencia de Bancos.*
- Asegurarse de que los procedimientos y controles de seguridad estén en línea con los requisitos establecidos en estos acuerdos.*

3. Capacitar al personal en seguridad de datos:

- Brindar formación regular al personal sobre las mejores prácticas de seguridad de la información.*
- Educar al personal sobre la importancia de proteger los datos personales y cómo identificar posibles riesgos de seguridad.*

4. Realizar auditorías de seguridad periódicas:

- Realizar auditorías regulares para evaluar la efectividad de las medidas de seguridad implementadas.*

- *Identificar y corregir cualquier vulnerabilidad o deficiencia en el tratamiento y la transferencia de datos.*

26. ¿Qué acciones deben tomarse ante un incidente de seguridad de datos personales? (Art. 26)

Las entidades bancarias tienen la responsabilidad de proteger los datos personales de sus clientes manteniendo su integridad, confidencialidad y disponibilidad para esto deben implementar las medidas técnicas, como administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Estas medidas deben ser proporcionales a la naturaleza y el tamaño de los datos personales tratados, así como al nivel de riesgo que implique su manejo.

Ante un incidente relevante que afecte de forma significativa la privacidad de los datos personales, la entidad bancaria debe comunicarle al regulador y a los afectados lo que ocurrió, qué datos se vieron comprometidos y qué medidas se tomaron para remediar la situación.

Contar con los protocolos de gestión de incidentes de seguridad que impliquen la adopción de medidas técnicas, administrativas y legales necesarias para protección de los datos personales, así como para prevenir, detectar y responder a los incidentes de violación.

Acciones recomendadas

- *Establecer dentro de su política, procedimiento o protocolos de Protección de datos personales de la entidad bancaria las acciones a tomar cuando se den incidentes de seguridad de la información tomando en consideración lo indicado en:*
 - *Acuerdo de Banca Electrónica Gestión del Riesgo de Tecnología de la Información (Acuerdo 06-2011, artículo 17)*
 - *Decreto 285 (artículo 37), que reglamenta la Ley 81 de Protección de datos personales donde se establece que se deben realizar los reportes de incidente de seguridad, en un término de tiempo de 72 horas.*

- *Las notificaciones a la Superintendencia de banco deben realizarse a través de los canales establecidos por el ente regulador.*
 - *Utilizar el Sistema de Reportes de Eventos e Incidentes de TI, que establece la SBP mediante el Link https://superbancos.gob.pa/reporte_grt/*
- *Las notificaciones hacia los clientes se manejan de acuerdo con lo establecido por cada entidad bancaria.*
- *Solicitar a los custodios de Base datos que cuenten con Políticas y procedimientos robustos que incluya mejores prácticas como lo establece las Norma ISO 27001 y 27701.*
- *Realizar auditorías periódicas para verificar el cumplimiento de las normas y políticas de protección de datos personales, así como para identificar y corregir las posibles deficiencias o riesgos.*
- *Capacitar y sensibilizar a colaboradores y personal tercerizado sobre la importancia de la protección de datos personales y las responsabilidades que implica su manejo.*

Sección 6. Formación y Capacitación

27. ¿Cómo debe ser la capacitación del oficial de protección de datos y su equipo? (Art. 23)

El Acuerdo 01-2022 en su Artículo 23 establece la importancia de la capacitación del OPD y su equipo para asegurar que puedan desempeñar sus funciones de manera efectiva. La capacitación debe ser integral, continua y específica para las necesidades de la entidad bancaria.

Acciones recomendadas

- **Capacitación integral en Protección de Datos Personales:** *La capacitación debe cubrir todos los aspectos de la protección de datos personales, incluyendo las normativas locales (como la Ley 81 y el Decreto Ejecutivo No. 285 de 2021), principios de protección de datos, derechos de los titulares, y medidas de seguridad de la información.*

Adaptar la capacitación a las necesidades específicas de la entidad bancaria, considerando las particularidades y riesgos asociados a la gestión de datos personales.

- **Actualización Continua:** *La capacitación debe ser continua y actualizada regularmente para incluir cambios en la legislación, nuevas amenazas a la seguridad de los datos y desarrollos tecnológicos relevantes.*
- **Colaboración Interdepartamental:** *Fomentar la colaboración con otras áreas del banco, como auditoría interna, riesgos, cumplimiento, tecnología y seguridad de la información, a través de sesiones de capacitación conjuntas con el objetivo de generar una comprensión y colaboración integradas en la protección de datos personales dentro de la organización.*
- **Evaluaciones y retroalimentación:** *Implementar evaluaciones para medir la efectividad de la capacitación y proporcionar retroalimentación al OPD, a su equipo o áreas involucradas directamente en la gestión de protección de datos personales.*

28. ¿Qué debe incluir el programa de capacitación a colaboradores? (Art. 23)

El programa de capacitación para los colaboradores de la entidad bancaria contribuye a que el personal esté preparado para proteger los datos personales de sus clientes y así cumplir con la normativa pertinente. Debe ser diseñado a mediano y largo plazo, con acciones específicas en el corto plazo para construir los conocimientos y comportamientos que se necesitan cimentar en la cultura organizacional.

A continuación, listamos los pasos clave para desarrollar el programa de capacitación:

- **Capacitación Formal:** *Se deben organizar sesiones de capacitación formales para el personal. Estas sesiones deben cubrir aspectos como la importancia de la protección de datos, los riesgos asociados a su divulgación no autorizada, y las prácticas recomendadas para proteger la información. La capacitación debe ser regular y actualizada para mantener a los colaboradores informados sobre las últimas amenazas y*

mejores prácticas, mediante sesiones presenciales, o utilizando una plataforma de entrenamiento virtual.

- **Concientización Continua:** *Además de la capacitación formal, es importante mantener una cultura de concientización continua sobre la protección de datos. Esto puede incluir la difusión de información relevante a través de boletines, revistas, seminarios web, tableros informativos y otros medios de comunicación interna.*
- **Pruebas:** *Se deben realizar pruebas y evaluaciones periódicas para verificar que el personal comprende y aplica correctamente las políticas y procedimientos de protección de datos. Por ejemplo, por medio de pruebas escritas o virtuales al final de cada capacitación. También se pueden realizar ejercicios de simulacros de incidentes, por su cualidad didáctica.*
- **Actualización Continua:** *Dado que las amenazas a la seguridad de los datos evolucionan constantemente, el Oficial de Protección de Datos y su equipo debe mantenerse al día con las últimas tendencias y tecnologías en la protección de datos.*

En cuanto a los temas clave para asegurar que todos los colaboradores estén bien informados y puedan aplicar medidas de seguridad efectivas, podemos mencionar los siguientes:

- **Políticas y procedimientos de protección de datos:** *deben formalizarse y comunicarse a toda la organización para asegurar que los colaboradores tengan conocimiento de cómo recopilar, almacenar, usar y eliminar datos de manera segura y conforme al régimen de protección de datos, en todo el ciclo de vida de los datos.*
- **Responsabilidades del personal:** *Es importante que los colaboradores comprendan sus responsabilidades en la protección de datos, incluyendo cómo tratar los datos personales de los clientes y cómo responder a solicitudes de derechos ARCOP.*
- **Privacidad por diseño:** *Enseñar a los colaboradores este enfoque proactivo que busca garantizar la protección de la privacidad y los datos personales desde el inicio del desarrollo de un producto, servicio o sistema.*

- **Leyes y regulaciones de protección de datos:** Es fundamental que los colaboradores estén familiarizados con el Acuerdo 01-2022 y el resto del régimen de protección de datos personales.
- **Cursos especializados:** Ofrecer capacitaciones especializadas para cada área. Por ejemplo: Recursos Humanos, Asesoría Legal, Auditoría, Junta Directiva.

Plan de seguridad de la Información orientado a la protección de los datos personales:

- **Seguridad de la información:** Debe incluirse cómo proteger la información en diferentes plataformas y dispositivos, incluyendo prácticas de seguridad de la red y el uso de contraseñas fuertes.
- **Prevención de robo de información:** Este tema debe cubrir cómo identificar y prevenir intentos de robo de información, incluyendo phishing y otros tipos de engaños.
- **Prevención de pérdida de datos (DLP):** Este tema debe cubrir cómo prevenir la pérdida accidental o intencional de datos confidenciales.

29. ¿Es necesario realizar las campañas de sensibilización a clientes, colaboradores y proveedores? (Art. 23, numeral 8)

*Según se indica en el artículo 23, numeral 8, el OPD debe coordinar el plan anual de capacitación para **colaboradores, directores y proveedores** de entidades bancarias; dentro del plan se pueden incluir campañas de sensibilización a través de los canales internos de la organización.*

*Se considera como buena práctica realizar campañas periódicas de sensibilización sobre protección de datos personales dirigida a los **clientes**, estas podrán estar alineadas a la estrategia de Seguridad de la Información y se pueden utilizar los canales de comunicación existentes. Por ejemplo, por medio del correo electrónico, el sitio web o de la banca en línea, redes sociales, revistas, mediante letreros o medios audiovisuales en sucursales, entre otros.*

En cuanto a los temas fundamentales para crear conciencia entre los clientes, colaboradores, directores y proveedores están los siguientes:

- a. **Educación sobre el Phishing y Otros Fraudes:** *Es fundamental educar a los clientes sobre cómo identificar y evitar estafas digitales, como el phishing. Esto incluye enseñarles a reconocer correos electrónicos, llamadas o mensajes sospechosos que intenten obtener información personal o bancaria.*
- b. **Uso de Contraseñas Robustas:** *Se debe recomendar a los clientes que utilicen contraseñas fuertes y únicas para sus cuentas bancarias y otros servicios en línea. Las contraseñas deben incluir una combinación de letras mayúsculas y minúsculas, números y símbolos.*
- c. **Verificación de Comunicaciones:** *Los clientes deben ser advertidos de que nunca deben proporcionar información personal o bancaria a través de correos electrónicos, llamadas o mensajes de texto, a menos que hayan iniciado la comunicación ellos mismos y estén seguros de la identidad de la otra parte.*
- d. **Implementación de Medidas de Seguridad:** *Los bancos deben asegurarse de que sus clientes estén utilizando canales seguros para realizar transacciones y acceder a sus cuentas. Esto incluye la verificación de dos factores y la implementación de medidas de seguridad avanzadas en sus plataformas en línea.*
- e. **Denunciar Posibles Fraudes:** *Los clientes deben ser animados a denunciar cualquier intento de fraude inmediatamente a su banco y a las autoridades pertinentes. Esto ayuda a prevenir futuros intentos de fraude y a proteger a otros clientes.*
- f. **Respuesta a Brechas de Seguridad:** *Explicar de forma sencilla y clara el procedimiento para denunciar incidentes relacionados con sus datos personales.*

Sección 7. Disposiciones Finales

30. ¿Cómo se gestionan los reclamos ante la Superintendencia? (Art. 27)

El Artículo 27 del Acuerdo 01-2022 establece el procedimiento que debe seguir un titular de datos personales cuando considere vulnerados sus derechos ARCO

(Acceso, Rectificación, Cancelación y Oposición) y desee presentar un reclamo ante la Superintendencia de Bancos.

Inicialmente, el titular de los datos debe presentar su reclamo ante la entidad bancaria responsable del tratamiento de los datos, el cual está obligado a atender la solicitud a través del Oficial de Protección de Datos (OPD) o el ejecutivo designado para estos fines.

Escenarios posibles en la gestión de reclamos

1. Solicitud ante el banco

- *El titular de los datos personales debe dirigir su solicitud, queja o controversia a la entidad bancaria.*
- *La entidad bancaria debe ofrecer medios y mecanismos accesibles y simplificados para que el cliente pueda ejercer sus derechos.*
- *La solicitud debe ser atendida dentro de los plazos establecidos por la normativa vigente (30 días).*

2. Escalamiento a la Superintendencia de Bancos

- *Si la entidad bancaria no responde en el tiempo correspondiente o el titular de los datos no está conforme con la respuesta, puede elevar el reclamo ante la Superintendencia de Bancos.*
- *El titular tiene un plazo de 30 días calendario para interponer su reclamo, contados a partir de la fecha en que recibió la respuesta de la entidad bancaria o desde el momento en que el banco no cumplió con atender la solicitud.*
- *La Superintendencia evaluará el caso conforme a los procedimientos establecidos en la Ley Bancaria y los Acuerdos bancarios aplicables.*

3. Escalamiento a la ANTAI

- *Si la Superintendencia de Bancos no emite una resolución en base al proceso administrativo correspondiente, el titular de los datos podrá presentar su reclamo ante la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI), de acuerdo con el Artículo 18 de la Ley No. 81 de 2019.*
- *Una vez la Superintendencia de Bancos emite y ejecuta su resolución, se agota la vía gubernativa, esto quiere decir que ya no se pueden*

presentar más recursos o apelaciones dentro de la misma institución gubernamental, sin perjuicio de los recursos legales en la vía contencioso-administrativa.

Acciones Recomendadas

- **Habilitar canales de atención accesibles:** *Implementar medios simplificados de comunicación (correo electrónico, formularios web, líneas telefónicas) para que los clientes pueden presentar sus reclamos de manera eficiente.*
- **Designar responsables claros:** *Asegurar que el Oficial de Protección de Datos (OPD) o un ejecutivo gestione las solicitudes de los titulares de datos personales.*
- **Establecer tiempos de respuestas claros:** *Garantizar que las solicitudes y reclamos se atienden en los plazos establecidos, evitando retrasos que puedan derivar en quejas antes la Superintendencia de Bancos.*
- **Capacitar al personal:** *Brindar formación continua a los equipos encargados de la gestión de reclamos en normativa de protección de datos y procedimientos internos.*
- **Documentar y registrar cada reclamo:** *Llevar un registro detallado de cada solicitud, su respuesta y la resolución final, asegurando trazabilidad en caso de auditorías o requerimientos de la Superintendencia.*
- **Facilitar información al cliente:** *Explicar claramente los procedimientos disponibles y sus derechos, incluyendo los plazos y pasos para elevar un reclamo ante la Superintendencia si no están conformes con a respuesta de la institución bancaria.*
- **Coordinar con la Superintendencia de Bancos:** *Mantener comunicación con la entidad reguladora para garantizar el cumplimiento de los procedimientos establecidos y responder oportunamente ante posibles requerimientos adicionales.*

31. ¿Cuál es el procedimiento de seguimiento, control y supervisión del acuerdo? (Art. 28)

El Artículo 28 del acuerdo 01-2022 establece que la Superintendencia de Bancos tiene la facultad de solicitar y verificar el cumplimiento de las normas de protección de datos personales por parte de las entidades bancarias. Esto implica la implementación de medidas técnicas, organizativas y de seguridad que garanticen la correcta protección de los datos personales tratados por las entidades bancarias.

Funciones de la Superintendencia de Bancos

- **Supervisión del cumplimiento normativo:** La Superintendencia podrá inspeccionar y evaluar si las entidades bancarias cumplen con los principios y estándares de protección de datos personales definidos en el Acuerdo y otras normativas relacionadas.
- **Solicitudes de Información y verificación:** Las entidades bancarias están obligadas a proporcionar toda la información que la Superintendencia de Bancos requiera para comprobar la correcta implementación de las medidas de protección de datos.
- **Revisión y evaluación de medidas de seguridad y políticas interna:** La Superintendencia verificará que los bancos cuenten con medidas de seguridad adecuadas, tanto técnicas como organizativas, para la protección de datos.

Además, evaluará si las políticas y procedimientos internos están actualizados y garantizan el cumplimiento de los derechos ARCO y la correcta gestión de incidentes de seguridad.

Acciones Recomendadas

- **Mantener documentación actualizada:** Garantizar que todas las políticas, procedimientos y registros relacionados con la protección de datos estén organizados y disponibles para ser presentados a la Superintendencia de Bancos cuando sean requeridos.
- **Establecer controles internos periódicos:** Implementar auditorías internas regulares para verificar el cumplimiento de las medidas técnicas, organizativas y de seguridad exigidas en el Acuerdo 01-2022. Además, como parte del seguimiento a la gestión integral de protección de datos, el OPD

podrá llevar un control (Excel o herramienta tecnológica) del cumplimiento de la normativa basado en la Ley 81, decreto y acuerdo 01-2022 así como reportes y tableros de seguimientos a los procesos establecidos.

- **Designar los responsables:** *Asegurar que el Oficial de Protección de Datos (OPD) y otros responsables internos supervisen continuamente el cumplimiento de la normativa y estén preparados para responder a cualquier requerimiento de la Superintendencia.*
- **Capacitar al personal bancario:** *Realizar entrenamientos periódicos en protección de datos personales, asegurando que los empleados comprendan sus responsabilidades y la importancia del cumplimiento legal.*
- **Actualizar las medidas de seguridad:** *Evaluar y mejorar continuamente los sistemas de protección de datos, asegurando que sean adecuados para mitigar riesgos y cumplir con los estándares exigidos.*

32. ¿Qué sanciones pueden aplicarse en caso de incumplimiento del acuerdo? (Art. 29)

El Artículo 29 del acuerdo 01-2022 establece que la Superintendencia de Bancos podrá imponer sanciones a las entidades bancarias que incumplan con las disposiciones del acuerdo y el régimen de Protección de Datos Personales. Estas sanciones se aplicarán según la gravedad de la falta y en conformidad con las normativas vigentes.

Tipos de Sanciones

- **Sanciones conforme a la Ley No. 81 de 2019 (art 39 – art 43)**
 - *Multas determinadas según la gravedad del incumplimiento.*
 - *Medidas correctivas impuestas para subsanar la falta en el tratamiento de datos personales.*
- **Procedimiento sancionatorio del Acuerdo No. 12-2015:**
 - *Se aplicará el procedimiento administrativo sancionador establecido en esta normativa, garantizando el debido proceso.*
 - *Las sanciones podrán incluir desde advertencias hasta la imposición de multas.*

- **Sanciones conforme a la Ley Bancaria (Título IV):**
 - *En casos donde se vulneren principios de confidencialidad bancaria, como la divulgación no autorizada de información de clientes, se podrán aplicar sanciones adicionales.*
 - *Estas pueden incluir penalizaciones económicas y otras medidas correctivas según lo estipulado en la Ley Bancaria.*

NOTA: Sin perjuicio de las sanciones anteriormente descritas existe la posibilidad de que las personas naturales puedan interponer demandas a las entidades bancarias por los daños y perjuicios ocasionados.

Acciones Recomendadas

- **Asegurar el cumplimiento normativo:** *Implementar controles internos estrictos para garantizar la correcta protección de los datos personales de los clientes.*
- **Capacitación continua:** *Sensibilizar a los empleados sobre las responsabilidades y consecuencias del incumplimiento del régimen de protección de datos.*
- **Auditorías internas:** *Realizar revisiones periódicas para detectar posibles incumplimientos y corregirlos antes de una supervisión externa.*
- **Fortalecer medidas de seguridad:** *Adoptar protocolos técnicos y organizativos que minimicen el riesgo de filtración o uso indebido de información.*
- **Gestión de incidentes:** *Establecer un procedimiento de respuesta rápida en caso de incidentes de seguridad relacionados con datos personales.*

33. ¿Cuándo entra en vigor el acuerdo y cuáles son sus disposiciones de vigencia? (Art. 30)

El Artículo 30 del Acuerdo 01-2022 establece que sus disposiciones entran en vigor a partir de su firma, lo que significa que desde ese momento las entidades bancarias deben cumplir con sus requisitos.

Sin embargo, dos artículos específicos contaron con un período de adecuación:

- *Artículo 22 (Designación del Oficial de Protección de Datos - OPD)*
- *Artículo 23 (Funciones y Responsabilidades del OPD)*

Para estos artículos, los bancos tuvieron un plazo de adecuación de 12 meses a partir del 24 de febrero de 2022, fecha en la que se firmó el acuerdo.

Esto permitió a las entidades bancarias contar con un período de transición para designar al OPD y establecer las funciones requeridas antes de la aplicación obligatoria de estos requisitos.

Acciones recomendadas

- **Revisión de cumplimiento actual:** *Verificar que todas las disposiciones del acuerdo ya hayan sido implementadas en la entidad bancaria.*
- **Evaluación del rol del OPD:** *Asegurar que el Oficial de Protección de Datos haya sido designado y cumpla con las funciones establecidas en los artículos 22 y 23.*
- **Auditorías internas:** *Realizar evaluaciones periódicas para confirmar que las obligaciones del acuerdo se han implementado de forma efectiva.*
- **Capacitación continua:** *Mantener al personal actualizado sobre las disposiciones del acuerdo y cualquier cambio normativo futuro.*
- **Documentación de cumplimiento:** *Contar con evidencia de la implementación del acuerdo en caso de requerimientos por parte de la Superintendencia de Bancos.*

ANEXOS

Anexo 1 - Hoja de ruta sugerida para el cumplimiento de la Ley 81, su reglamentación y el acuerdo 01-2022

HOJA DE RUTA LEY 81

IMPLEMENTACIÓN ENTIDADES BANCARIAS



Anexo 2 - Artículo 15. Registro de transferencia de datos.

A continuación, la descripción de los campos mínimos que deben incluirse dentro del registro de transferencia de datos personales:

Registro de Transferencias – Requisitos mínimos			
	REQUISITO - columnas	DEFINICIÓN	Ejemplo – entrega de base de datos para mensajería externa de tarjetas
1	Identificación o nombre de la base de datos (descripción funcional)	Nombre funcional de acuerdo con el tipo y propósito de la base de datos.	- Nombre del Archivo: Control de tarjetas para mensajería_15marzo2025
2	Identificación o nombre del responsable de la Base de Datos (dueño de la información interno)	Responsable a nivel funcional dentro de la organización. Es el dueño de la información, es el área encargada del tratamiento de los datos, es la que recopila y se encarga de darle mantenimiento.	- Responsable Base de datos: Gerente de Operaciones de tarjetas
3	Naturaleza de los datos personales que contiene la base de datos	Indicar si el dato personal dentro de la base de datos es de tipo general o sensible como mínimo, pero en caso de que la entidad adicional tenga otras clasificaciones las puede incluir dentro del registro.	- Categoría de datos utilizados: Datos de identificación, contacto, dirección
4	Condiciones de legitimación aplicables	Indicar la o las condiciones de licitud que le permiten al responsable realizar el tratamiento de los datos personales contenidos en esa base de datos, tomando como referencia la normativa aplicable, como la Ley 81 de 2019 y el Acuerdo 1-2022, que respaldan el tratamiento de los datos.	- Base legal: Consentimiento y/o relación contractual NOTA: incluir las más relevantes: consentimiento – relación contractual – obligación legal – interés legítimo
5	Finalidades del tratamiento	Detallar las finalidades del tratamiento de los datos personales contenidos en esa base de datos (campo abierto).	- Entrega física de tarjetas de crédito o débito a través de un servicio tercerizado.

6	Procedimientos de obtención y tratamiento de datos		
6.1	Método de Obtención	Medios manuales y medios digitales. Fuente de donde se obtienen los datos personales: directamente del titular, bases de datos públicas, terceros autorizados, etc. Métodos utilizados para recolectar los datos: formularios físicos o digitales, interacciones con el sitio web, llamadas, etc.	<ul style="list-style-type: none"> - Directamente del titular de los datos - A través de formulario digital en página web.
6.2	Procedimientos de tratamiento de datos	Nombre del procedimiento asociado al tratamiento de datos personales.	<ul style="list-style-type: none"> - Procedimiento de otorgamiento de tarjetas de crédito/débito.
7	Plazo de conservación	Indicar los plazos de conservación para los datos personales contenidos en la base de datos, de acuerdo con las políticas internas de la organización.	<ul style="list-style-type: none"> - Mientras dure la relación contractual con el proveedor de servicios de mensajería.
8	Destino de los datos	Nombre del proveedor o entidad a la cual se le van a entregar los datos y los proveedores de estos, a los que posiblemente le puedan transferir los datos con posterioridad.	<ul style="list-style-type: none"> - Proveedor XX, S.A. (razón social del proveedor)
9	Persona de contacto del destinatario	Nombre de la persona de contacto en el proveedor.	<ul style="list-style-type: none"> - Lic. Juan Pérez (representante legal o persona designada)
10	Medidas técnicas y organizativas de seguridad	Características del canal seguro por el cual se comparte la información (por ejem: goanywhere, SFTP, VPN, y otros). También los protocolos internos para garantizar la seguridad de los datos (dar un breve resumen). Otras medidas de seguridad que podrían aplicarse son: <ul style="list-style-type: none"> - Aplicación de cookies, identificadores digitales y otros mecanismos de monitoreo de actividad en línea. 	<ul style="list-style-type: none"> - El Excel es compartido al proveedor a través de un proceso automatizado de GoAnyWhere y es colocado en una carpeta segura con acceso restringido solo a los usuarios que son parte del proceso.

		- Plan de acción en caso de fuga, pérdida o acceso no autorizado a los datos personales.	
11	Procedimientos para atención y respuesta del ejercicio de los derechos de los titulares de datos	Indicar si la atención de las solicitudes de los Derechos ARCOP la ejecuta el banco o el proveedor/tercero	- El proveedor no realizará atención de los derechos ARCOP, proceso lo sigue ejecutando el banco en sucursales físicas o virtuales.
12	Descripción técnica de la base de datos	Nombre técnico de la BD, tipo de datos (texto, numérico, alfanumérico).	- Nombre de Base de datos: BD_registro_mensajeríaTDC - Tipo de datos: Texto o alfanumérico
13	Identificación y período de todas las personas que han ingresado a los datos personales	El responsable o custodio de los datos debe llevar un registro de los usuarios que ingresan a la base de datos (fecha, hora, nombre de usuario) y mantener la bitácora de acceso de al menos 15 días.	- Dd/mm/aaa, hora, nombre de usuario
14	Cantidad de Registros	Total de clientes o titulares de los datos que forman parte de la base de datos compartida.	- 150 registros diarios/incremental

Anexo 3. Aviso de Privacidad

Detalle de cada punto del aviso de privacidad que se debe completar a través de ejemplos.

Elemento informativo / Actividades para su cumplimiento	Ejemplo de texto
Identidad del responsable del tratamiento de datos	La entidad responsable del tratamiento de sus datos personales es <i>[Nombre de la empresa]</i> , ubicada en <i>[Dirección física]</i> , con correo electrónico de contacto <i>[correo electrónico]</i> .
Marco legal aplicable	La empresa cumple con las normativas de protección de datos establecidas en la [Ley aplicable] , su reglamento y demás normas concordantes de la <i>[País]</i> .
Definiciones clave	Para efectos del presente aviso, se definen los términos esenciales como "datos personales", "tratamiento de datos", "responsable del tratamiento", entre otros, según la legislación vigente.
Finalidad del tratamiento de datos personales	La información personal que recopilamos será utilizada exclusivamente para la prestación de servicios, gestión de contratos, cumplimiento de obligaciones legales y envío de comunicaciones comerciales, siempre con el consentimiento del titular.
Base legal del tratamiento de datos	La empresa trata los datos personales en cumplimiento de obligaciones contractuales, consentimiento explícito del titular, interés legítimo y disposiciones legales aplicables.
Datos personales que se recopilan	Se recopilan datos de identificación, contacto, financieros y cualquier otra información relevante para la prestación de servicios y cumplimiento de normativas regulatorias.
Fuente de obtención de los datos	La recopilación de datos se realiza a través de formularios en línea, contratos físicos, aplicaciones móviles y otros medios digitales o presenciales.
Transferencia de datos a terceros	Los datos pueden ser compartidos con entidades afiliadas, reguladores, proveedores de servicios y autoridades competentes en cumplimiento de la legislación vigente.
Transferencias internacionales de datos	En caso de ser necesario, los datos pueden ser transferidos a países que garanticen un nivel de protección adecuado según la normativa aplicable.
Periodo de conservación de los datos	Los datos personales serán almacenados durante <i>[X años]</i> después de la finalización de la relación contractual o el tiempo requerido por la legislación vigente.
Derechos del titular de los datos (Derechos ARCO)	Los titulares pueden ejercer sus derechos de acceso, rectificación, cancelación y oposición mediante una solicitud enviada a <i>[correo electrónico]</i> o en nuestras oficinas.
Proceso para ejercer derechos ARCO	Para ejercer estos derechos, el titular deberá presentar una solicitud formal, acreditando su identidad, y la empresa responderá en un plazo de <i>[X días]</i> hábiles.

Retiro del consentimiento	El titular puede revocar su consentimiento en cualquier momento sin efectos retroactivos, enviando una solicitud a [correo electrónico].
Medidas de seguridad para la protección de datos	La empresa implementa medidas de seguridad técnicas y organizativas para proteger los datos contra accesos no autorizados, pérdida o alteración.
Uso de tecnologías de rastreo (cookies y otros identificadores)	Se utilizan cookies y herramientas de seguimiento para mejorar la experiencia del usuario en nuestras plataformas digitales. Puede gestionar sus preferencias a través de la configuración de su navegador.
Autoridad de control en protección de datos	En caso de dudas o reclamaciones, el titular puede dirigirse a la [Entidad reguladora de protección de datos] de [País].
Modificaciones al aviso de privacidad	La empresa se reserva el derecho de modificar este aviso en cualquier momento. Las actualizaciones serán publicadas en [sitio web oficial].

Otros enlaces relacionados a la formalización del AVISO DE PRIVACIDAD

- https://www.amda.mx/wp-content/uploads/docs/avisosdeprivacidad/se_privacidad-guia_sep11.pdf
- <https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/ GuiaAP-RRHH.pdf>

Anexo 4. Ficha Técnica / Manual de Protección de Datos

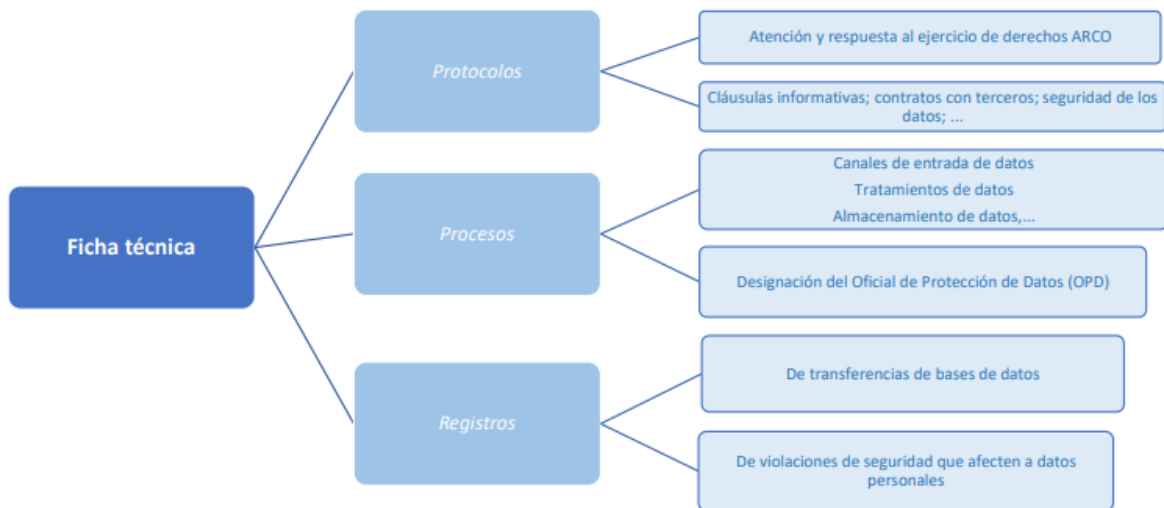
La Ley 81 sobre Protección de Datos Personales define en el artículo 4, numeral 13, la *Ficha Técnica* como:

“Documento que contiene los registros, protocolos y reglas, relacionados al almacenamiento y tratamiento de los datos personales”

En el Acuerdo 01-2022, artículo 4 se define la Ficha Técnica como:

*“Documento que contiene los registros, protocolos y reglas, relacionados al almacenamiento y tratamiento de los datos personales, **entendiéndose para efectos del presente acuerdo como las políticas y procedimientos adoptados por el banco**”.*

De este modo, la ley traslada al responsable o custodio de la base de datos la obligación de elaborar los registros, protocolos y reglas o procedimientos de gestión y transferencia segura de los datos personales que sean necesarios en el desarrollo de su actividad ligada al tratamiento de los datos personales. En el gráfico siguiente se recoge lo que podría ser un ejemplo del contenido principal de esta Ficha Técnica:



(Pou)

Anexo 5. Casos de uso / Consultas generales

Caso de Uso 1: ¿Cuánto tiempo se debe conservar la información de clientes?

- **Escenario:**
Una institución quiere destruir expedientes físicos de clientes. Se pregunta si debe conservarlos 5 o 7 años.
- **Respuesta consensuada:**
 - *El plazo depende del tipo de documento: Ley 23, APC, etc.*
 - *Por ejemplo, documentos APC: 1 año si no es cliente, 5 si lo es.*
 - *Los 7 años se interpretan como el periodo posterior al plazo legal de conservación de los expedientes físicos de los clientes cuando haya finalizado la relación contractual (no tiene ningún producto bancario activo) donde ya no se debe comunicar o transferir los datos personales.*
- **Guía práctica:**
Revisar normativa aplicable por tipo de documento. Mantener una política de retención y destrucción clara, documentada y aprobada según lineamientos de cada entidad bancaria.

Caso de Uso 2: ¿El proveedor de facturación electrónica es custodio de datos?

- **Escenario:**
Una empresa utiliza un Proveedor Autorizado Calificado (PAC) para facturación electrónica y quiere saber si este proveedor es custodio de datos o solo un proveedor de servicios bancarios.
- **Respuesta:**
 - *Sí, se considera custodio de datos.*
 - *Se debe gestionar un DPA (Data Processing Agreement) y NDA (Non Discloser Agreement)/Acuerdo de Confidencialidad*
 - *Solo se documenta el registro de transferencia una vez, pero se hace DPIA (evaluación de impacto) incluyendo canal, almacenamiento, frecuencia, etc.*
- **Guía práctica:**
Clasificar correctamente al tercero (procesador/custodio), firmar DPA, y documentar DPIA.

Caso de Uso 3: Eliminar datos de referencias personales

- **Escenario:**
Un cliente dejó referencias personales. Al contactarlas por deuda, una referencia dice que no tiene relación con el cliente y pide eliminar su dato. ¿Se debe eliminar el dato de esa referencia?

- **Respuesta:**
 - *Si no hay consentimiento expreso de la referencia personal del cliente, se debe eliminar, ya que estos no son clientes de la entidad bancaria.*
 - *Algunas entidades bancarias los eliminan inmediatamente al solicitarlo, sin requerir completar formularios adicionales de derechos ARCOP.*

- **Guía práctica:**
Incluir cláusulas claras o disclaimer sobre uso limitado de datos de terceros. Dejar establecido procedimentalmente que si una referencia personal solicita se elimina de los registros de la entidad será ejecutada la solicitud de forma inmediata.

Caso de Uso 4: ¿Es necesario consentimiento firmado para clientes antiguos?

- **Escenario:**
Entidad bancaria con cuentas de ahorro, corriente o plazo fijo, sin nuevos productos posterior a la entrada en vigencia de la ley, envió formulario de consentimiento, pero pocos lo han devuelto firmado. ¿Es necesario contar con el consentimiento firmado por clientes antiguos?

- **Respuesta:**
 - *Si ya existe un contrato entre las partes, esto es la base legitimadora para el tratamiento de datos personales de clientes antiguos que se realiza.*
 - *Como buena práctica, en la actualización regulatoria se puede gestionar el consentimiento explícito, informado e inequívoco de estos clientes.*
 - *Es recomendable notificar del aviso de privacidad informando sobre sus derechos y finalidades en el uso de sus datos personales.*

- **Guía práctica:**
Verificar si ya hay base legal (contrato). Enviar avisos de privacidad como complemento.

Caso de Uso 5: ¿Qué hacer con datos ya transferidos al ejercer cancelación?

- **Escenario:**
Cliente ejerce derecho de cancelación, pero sus datos ya fueron compartidos con fiduciarias u otros terceros. ¿Se le pide al tercero que cancele los datos también?
- **Respuesta:**
 - *Sí, si es técnicamente viable y está contemplado contractualmente.*
 - *Se debe establecer en el contrato cuánto tiempo el tercero mantendrá los datos y cómo se evidenciará su eliminación.*
- **Guía práctica:**
Incluir cláusulas de eliminación de datos en contratos con terceros. Verificar cumplimiento tras ejercicio de derechos. De ser posible definir contractualmente los puntos claves de cómo se eliminarán los datos por parte de los terceros y quienes certificarán la misma.

Caso de Uso 6: ¿Se deben marcar de forma especial los datos de personas discapacitadas?

- **Escenario:**
Una entidad bancaria pregunta si los datos de personas con discapacidad requieren tratamiento especial dentro del sistema. ¿Deben los datos de una persona discapacitada tener algún marcaje o separación especial en las bases de Datos?
- **Respuesta:**
 - *No se requiere tratamiento diferente.*
 - *Lo importante es tener claro quién está autorizado para actuar por la persona o en su representación (representante legal o tutor).*
- **Guía práctica:**
Tratar los datos personales según el estándar establecido cumpliendo con el régimen de protección de datos vigente y mejores prácticas internacionales, pero asegurar respaldo documental para interacciones con terceros que actúen en representación del titular de los datos (derechos ARCOP).

Caso de Uso 7: ¿Qué se debe hacer si las personas que están como referencias personales no desean que se utilice su información?

- **Escenario:**
Una persona registrada como referencia personal por un cliente exige eliminar sus datos del banco. ¿Se debe eliminar el dato de esa referencia si no lo autorizó?
- **Respuesta:**

- *Sí, si la referencia no dio consentimiento explícito a la entidad bancaria.*
- *No se debe conservar ni usar el dato sin base legal.*
- **Guía práctica:**
Implementar disclaimers en formularios donde el cliente confirme que ha notificado a los titulares que coloca como referencias personales en la entidad bancaria; adicional, en el aviso de privacidad indicar de forma sencilla el uso de los datos de referencias personales.

Caso de Uso 8: ¿Puede un banco ofrecer productos a miembros de la Junta Directiva de clientes jurídicos?

- **Escenario:**
Cientes jurídicos dan información de sus dignatarios durante el proceso de apertura de cuenta y la entidad bancaria se pregunta si se puede usar para marketing. ¿Se puede contactar para ofrecer productos del banco a miembros de la JD de clientes jurídicos?
- **Respuesta:**
 - *Sí, siempre y cuando se tenga el consentimiento previo del dignatario para tratar sus datos y ofrecer otros productos.*
 - *Se debe mantener la trazabilidad y la evidencia de dicha autorización.*
- **Guía práctica:**
Evitar usar datos de dignatarios o terceros para fines distintos al original sin su consentimiento. Dentro de los procesos de apertura de cuenta deben evaluar la inclusión de cláusulas o formularios de consentimiento para los dignatarios.

Caso de Uso 9: ¿Qué documentación exige la SBP en auditorías?

- **Escenario:**
Varias instituciones comentan sobre auditorías de la Superintendencia de Bancos. ¿Qué documentación les pide la SBP en auditorías sobre protección de datos?
- **Respuesta:**
La documentación solicitada va a depender del alcance del auditoria que se esté realizando y del auditor encargado de la misma. Como referencia, sin limitarse dejamos aquí algunos de los documentos requeridos:
 - *Manuales PDP*

- *Políticas y procedimientos*
 - *Consentimiento informado*
 - *Evidencias de derechos ARCO*
 - *Matriz de riesgos operativos*
 - *Descriptores de funciones del OPD*
-
- ***Guía práctica:***
Mantener una carpeta actualizada con la documentación definida dentro del Manual o Ficha técnica de la gestión de Protección de datos personales de la entidad bancaria.

Anexo 6. Matriz de Riesgos de Protección de datos.

Guía metodológica para el análisis de riesgos de datos personales

Elemento informativo / Actividades para su cumplimiento	Descripción
Contexto del tratamiento	Acceso no autorizado a datos personales de clientes por parte de personal interno.
Identificación de activos	Detectar los sistemas, archivos, software y procesos que intervienen en el tratamiento de datos personales.
Amenazas y vulnerabilidades	Identificar los factores que pueden afectar la seguridad (fallas técnicas, errores humanos, accesos no autorizados, etc.).
Evaluación del impacto	Estimar el grado de afectación a los derechos y libertades de los titulares si se materializa una amenaza (daño reputacional, discriminación, etc.).
Probabilidad de ocurrencia	Determinar qué tan probable es que ocurra un incidente. Puede clasificarse como baja, media o alta, según historial, controles y contexto.
Nivel de riesgo	Resultado de combinar impacto y probabilidad. Se expresa generalmente en una escala (bajo, medio, alto) y permite priorizar.
Controles existentes	Identificar medidas ya implementadas: cifrado, acceso restringido, backups, políticas, etc.
Riesgo residual	Riesgo que permanece luego de aplicar los controles. Es clave para determinar si se necesita implementar nuevas medidas.
Medidas correctoras o mitigadoras	Acciones planificadas para reducir o eliminar riesgos residuales. Deben incluir responsables, plazos, y recursos asignados para su implementación.
Revisión y actualización periódica	Establecer una frecuencia de revisión de la matriz (ej. anual, semestral) o tras cambios significativos en procesos, tecnologías o normativa.

Documento de referencia:

<https://www.uclm.es/-/media/Files/A01-Asistencia-Direccion/A01-023-Vicerrectorado-Politica-Cientifica/ComiteCienciasSociales/Datos/Analisis-y-gestion-de-riesgos.ashx?la=en>

Tipo de Amenaza	Amenaza	Riesgo	Control	Probabilidad	Impacto	Riesgo residual
Acceso ilegítimo a los datos	Fuga de información	Terceras personas acceden a los datos vulnerando su confidencialidad	Acceso a usuarios autorizados mediante uso de credenciales y MFA	Despreciable – Valoración: 1	Significativo – Valoración: 3	Medio – Valoración: 3
	Operaciones de tratamiento no autorizadas	Uso ilegítimo de los datos que vulneran los derechos de los interesados	Acceso a usuarios autorizados mediante uso de credenciales y MFA	Despreciable – Valoración: 1	Limitado – Valoración: 2	Bajo – Valoración: 2
Modificación no autorizada de los datos	Ataque de software malicioso (Ciberataque)	Se modifican los datos perdiendo su integridad	Utilización de sistema antivirus de última generación	Despreciable – Valoración: 1	Limitado – Valoración: 2	Bajo – Valoración: 2
	Operaciones que modifican datos de forma ilegítima	Uso ilegítimo de los datos que vulneran los derechos de los interesados	Acceso a modificar datos solo a perfiles de usuario autorizados	Despreciable – Valoración: 1	Significativo – Valoración: 3	Medio – Valoración: 3
Indisponibilidad de los datos	Corte del suministro eléctrico que impide el acceso	Imposibilidad de acceder a los datos porque no están disponibles	Utilización de sistemas de alimentación ininterrumpida	Despreciable – Valoración: 1	Limitado – Valoración: 2	Bajo – Valoración: 2
	Ciberataque que impide acceder a los datos	Imposibilidad de acceso a los datos porque no están disponibles	Utilización de sistema antivirus de última generación	Limitada – Valoración: 2	Significativo – Valoración: 3	Medio – Valoración: 6

Participantes de la Comisión de Protección de Datos Personales

Etapa 1 – Grupos de trabajo para análisis e interpretación de los artículos del Acuerdo 001-2022.

Grupo #1: Rolando Rivera (Banisi)/ Orlando S. González (Banco Occidente)

Grupo #2: Isabel Lopez (Multibank)/ Roderick Pedreschi (BHD Bank)

Grupo #3: Lorenzo Escudero (BNP) /Angélica Espinosa (Banistmo)

Grupo #4: Víctor Antinori (BNP)/ Aris Guerra (Banco Aliado)

Grupo #5: Milagros Manzzo (BAC) / Ken Chen (Multibank)

Grupo #6: Jorge Contreras (BI Bank)/ Daisy Alvarez (Banco Pichincha - Q.E.P.D.)

Etapa 2 – Grupo reducido encargado de unificar toda la información y estructurarla.

Tatiana Rodríguez –Metrobank

Rolando Rivera – Banisi

Aris Guerra – Banco Aliado

Rolando Armuelles – BNP

Isabel López - Multibank

Referencias

- [Ley 81, 26 marzo 2019](#)
- [Decreto 285, 28 mayo 2021](#)
- [Acuerdo Bancario 001-2022](#)



ASOCIACIÓN BANCARIA DE PANAMÁ

Avenida Samuel Lewis, Torre Canaima– Piso 15
(al lado del Santuario Nacional)
Tel: (507) 263-7044
Telefaxes: (507) 263-7783 / 223-7630
Email: info@asociacionbancaria.com
Apartado Postal: 08160-0805, Rep. de Panamá

@abpanama

