POLÍTICA N.º 65: **PROTECCIÓN DE DATOS PERSONALES**

DIRECCIÓN RESPONSABLE: **DESPACHO SUPERIOR**

FECHA DE EMISION: **10 DE OCTUBRE DE 2022**

Con el propósito de dar fiel cumplimiento a las disposiciones en relación con la **Política N.º 65** sobre **Protección de datos personales**; en donde de acuerdo con la Ley 81, del 26 de marzo de 2019, se entiende por dato personal cualquier información concerniente a personas naturales, que las identifica o las hace identificables; en este sentido, Superintendencia de Bancos establece lo siguiente:

I. Objetivo:

- Promover el desarrollo eficiente del tratamiento y protección de datos personales de clientes, visitantes, proveedores, titulares de los datos gestionados por SBP, así como de los colaboradores de la institución, de forma que estos datos se traten en base a los términos que establece la Ley 81, del 26 de marzo de 2019 y su reglamentación mediante el Decreto N.º 285 de mayo de 2021.
- Dar a conocer los datos que son capturados y el tratamiento que la Superintendencia de Bancos efectúa a estos.
- Brindar a los propietarios de los datos personales un mecanismo para ejercer su derecho de acceso, rectificación, cancelación, oposición y portabilidad.

II. Alcance:

La presente política está dirigida a establecer los requerimientos mínimos de seguridad establecidos por la Superintendencia de Bancos para la gestión y tratamiento de todos los datos personales, así como de las bases de datos que contengan datos personales y sobre los cuales Superintendencia de Bancos actúa como responsable.

Todo tratamiento de datos personales deberá ser realizado en los términos, condiciones y fines establecidos en las autorizaciones de tratamientos entregadas a Superintendencia de Bancos por el titular de los datos personales.

La política debe ser conocida y aplicada por los colaboradores, clientes, proveedores y titulares de los datos personales gestionados por Superintendencia de Bancos, tiene como finalidad:

- Dar a conocer los datos personales que se recolectan y el tratamiento que Superintendencia de Bancos aplica a este conforme lo establece la Ley.
- Proporcionar a los titulares de los datos personales gestionados, un instrumento que les permita conocer los derechos de acceso, rectificación, cancelación, oposición y portabilidad.

Todas las bases de datos de Superintendencia de Bancos que gestionen datos personales serán inventariadas y registradas de conformidad con lo dispuesto en la ley y su reglamentación.

III. Términos y definiciones:

- Almacenamiento de datos: Conservación o custodia de los datos personales de colaboradores, proveedores y clientes en una base de datos establecida en cualquier medio provisto, incluido el de la tecnología de la información y la comunicación por parte de esta Superintendencia o un proveedor de servicios.
- Aviso de privacidad: Comunicación generada por la Superintendencia dirigida al interesado para el tratamiento de sus datos personales, mediante la cual se le comunica acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas, las finalidades del tratamiento que se pretende dar a los datos personales y demás elementos que deberá informar al cliente al momento de la obtención de los datos.
- Base de datos personales: Conjunto ordenado de datos personales, cualquiera que sea la forma o modalidad de su creación, organización o almacenamiento, que permite relacionar los datos de los colaboradores, proveedores y clientes entre sí, así como realizar cualquier tipo de tratamiento o transmisión de estos por parte de su custodio.
- Consentimiento: Manifestación de la voluntad libre, específica, informada e inequívoca del titular de los datos, mediante la cual se efectúa el tratamiento de estos.
- Custodio de la base de datos: responsable del tratamiento de los datos personales de los colaboradores, proveedores y clientes y le compete la custodia y conservación de la base de datos.
- Dato personal: Cualquier información concerniente a los colaboradores, proveedores y clientes que los identifica o los hace identificable.
- Dato sensible: Aquel que se refiera a la esfera íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, a la preferencia u orientación sexual, datos genéticos o datos biométricos, entre otros, sujetos a regulación y dirigidos a identificar de manera inequívoca a una persona natural.
- Derechos ARCO: Derechos irrenunciables básicos de los titulares de los datos, identificados como: derecho de acceso, rectificación, cancelación, oposición y portabilidad, de conformidad con los términos definidos en la Ley **N.º** 81 de 26 de marzo de 2019 y el Decreto Ejecutivo **N.º** 285 de 28 de marzo de 2021.
- Responsable del tratamiento de los datos: es la entidad a la que le corresponde las decisiones relacionadas con el tratamiento de los datos personales y que determina los fines, medios y alcance, así como cuestiones relacionadas con estos, en este caso es la Superintendencia.
- Titular de los datos: Persona natural a la que se refieren los datos personales.
- Tratamiento de datos: Cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permita recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, asociar, disociar, comunicar, ceder, intercambiar, transferir, transmitir o cancelar datos, o utilizarlos en cualquier forma.

IV. Principios:

Los principios generales en los cuales se inspiran y rigen la protección de datos de carácter personal, en cuanto a la interpretación y aplicación de la normativa, son:

- *Principio de lealtad*: los datos personales deberán recabarse sin engaño o falsedad y sin utilizar medios fraudulentos, desleales o ilícitos.
- *Principio de finalidad*: los datos personales deben ser recolectados con fines determinados y no ser tratados posteriormente para fines incompatibles o distintos para los cuales se solicitaron, ni conservarse por tiempo mayor del necesario para los fines de tratamiento.
- *Principio de proporcionalidad*: solo deberán ser solicitados aquellos datos adecuados, pertinentes y limitados al mínimo necesario en relación con la finalidad para la que son requeridos.
- *Principio de veracidad y exactitud*: los datos de carácter personal serán exactos y puestos al día de manera que respondan con veracidad a la situación actual del propietario del dato.
- *Principio de seguridad de los datos*: los responsables del tratamiento de los datos personales deberán adoptar las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos bajo su custodia, principalmente cuando se trate de datos considerados sensibles, e informar al titular, lo más pronto posible, cuando los datos hayan sido sustraídos sin autorización o haya indicios suficientes de que su seguridad ha sido vulnerada.
- *Principio de transparencia*: toda información o comunicación al titular de los datos personales relativa al tratamiento de estos deberá ser en lenguaje sencillo y claro, y mantenerlo informado de todos los derechos que le amparan como titular del dato, así como la posibilidad de ejercer los derechos ARCO.
- *Principio de confidencialidad*: todas las personas que intervengan en el tratamiento de datos personales están obligadas a guardar secreto o confidencialidad respecto de estos, incluso cuando hayan finalizado su relación con el titular o responsable del tratamiento de datos, impidiendo el acceso o uso no autorizado.
- *Principio de licitud*: para que el tratamiento de un dato personal sea lícito, deberá ser recolectado y tratado con el consentimiento previo, informado e inequívoco del titular del dato o por fundamento legal.
- *Principio de portabilidad*: el titular de los datos tiene derecho a obtener de parte del responsable del tratamiento una copia de los datos personales de manera estructurada en un formato genérico y de uso común.

V. Derechos de los titulares (Derechos ARCO):

Se reconocen como derechos irrenunciables básicos, los derechos que tienen los titulares de datos personales, como:

- *Derecho de Acceso*: obtener sus datos personales que se encuentren almacenados o sujetos a tratamiento en las bases de datos de la Superintendencia de Bancos, además de conocer el origen y la finalidad para los cuales han sido recabados.
- D*erecho de Rectificación*: solicitar rectificación o la corrección de los datos personales que sean incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes.
- D*erecho de Cancelación*: solicitar la eliminación o cancelación de sus datos personales que estén incorrectos, sean irrelevantes, incompletos, desfasados, inexactos, falsos.
- D*erecho de Oposición*: por motivos fundados y legítimos relacionados con una situación en particular, podrá negarse a proporcionar sus datos personales o a que sean objeto de determinado tratamiento, así como a revocar su consentimiento.
- D*erecho de Portabilidad*: obtener una copia de los datos personales de manera estructurada, en un formato genérico y de uso común.

VI. Limitación del derecho

Sin perjuicio de las limitaciones indicadas en los artículos del Decreto 285 que reglamenta la Ley 81 de 2019, podrá limitarse el ejercicio de los derechos del titular de los datos personales, en cualquiera de los siguientes casos:

- Cuando el tratamiento sea necesario para el cumplimiento de un objetivo del interés público.
- Cuando el tratamiento impida o entorpezca el debido trámite dentro de un proceso administrativo o judicial o por seguridad del Estado.
- Cuando sea necesario para el ejercicio de las funciones propias de las autoridades públicas.
- Cuando sea solicitado por las autoridades judiciales competentes para el aseguramiento del cumplimiento de la Ley, con las condiciones previstas en la Ley 81 de 2019.
- Cuando el responsable del tratamiento acredite tener motivos legítimos para que el tratamiento prevalezca sobre los intereses, los derechos y las libertades del titular.
- Cuando el tratamiento sea necesario para el cumplimiento de una ley.
- Cuando los datos personales sean necesarios para el mantenimiento o cumplimiento de una relación jurídica o contractual.

Los datos sensibles no serán objeto de transferencia, excepto en los casos siguientes:

- Cuando el titular haya dado su autorización explícita, salvo en los casos que por Ley no sea requerido el otorgamiento de dicha autorización.
- Cuando sea necesario para salvaguardar la vida del titular y se encuentre física o jurídicamente incapacitado. En estos casos, los acudientes, curadores o quienes tengan la tutela deben dar la autorización.
- Cuando se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso con autorización judicial competente.
- Cuando tenga una finalidad histórica, estadística o científica. En este caso, deberán adoptarse las medidas conducentes a disociar la identidad de los titulares.

VII. Plazos para facilitar la información y autorización del titular:

Cuando los datos sean proporcionados por el titular, la información se facilitará en el momento de la recogida de los datos, ya sea de forma presencial o virtual.
Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior. Se entenderá que la autorización cumple con estos requisitos cuando se manifieste (i) por escrito, (ii) aceptación a mensajes o políticas de privacidad a través del sitio web, o en diferentes aplicaciones que mantenga la institución.

VIII. Personas a quienes se les puede suministrar la información

La información que reúna las condiciones establecidas en la ley, podrá ser suministrada a las siguientes personas:

a) A los titulares, sus causahabientes o sus representantes legales.
b) A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.
c) A los terceros autorizados por el Titular o por la ley.

IX. Procedimiento y formularios para facilitar la información:

El titular de los datos o quien lo represente podrá ejercer sus derechos y solicitar a la Superintendencia de Bancos información, la cual deberá ser proporcionada en un plazo no mayor de diez (10) días hábiles, a partir de la fecha de presentación de la solicitud.

Clientes/proveedores:

- Completar el formulario de solicitud correspondiente, dependiendo el derecho a ejercer.
- Enviar formulario firmado y agregar documento de identificación, ambos escaneados a través del correo electrónico datospersonales@superbancos.gob.pa.
- Superintendencia de Bancos tendrá un plazo de 2 días hábiles para acusar de recibido a la solicitud. (explicar sobre los términos)
- Tiempo de respuesta (para solicitar información de sus datos, su eliminación u oponerse a algún tratamiento): menor o igual a 8 días hábiles, a partir de la fecha de solicitud.
- Tiempo de respuesta (para modificar datos errados, inexactos, equívocos o incompletos): 5 días hábiles siguientes a la solicitud de modificación.
- El trámite es gratuito.
- Superintendencia de Bancos entregará información electrónicamente (correo electrónico), si el titular solicita que la información le sea suministrada en USB deberá suministrar este dispositivo al cual será transferida la información o él asumir el costo de esta solicitud. El dispositivo proporcionado por el titular de los datos debe ser suministrado sin formato, ni información.
- Si una vez realizada la solicitud, la Institución no se pronuncia sobre la solicitud del titular de datos personales dentro de los términos establecidos, el titular de los datos personales tendrá derecho a recurrir a la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI).
- El titular tendrá, además, derecho a exigir que se eliminen sus datos personales cuando su almacenamiento carezca de fundamento legal, cuando no hayan sido expresamente autorizados o cuando estuvieran caducos.

Colaboradores o excolaboradores:

- Superintendencia de Bancos deberá indicar al titular, el tratamiento de sus datos desde el inicio de la relación contractual.
- Completar el formulario de solicitud correspondiente, dependiendo el derecho a ejercer.
- Enviar formulario firmado y agregar documento de identificación, ambos escaneados a través del correo electrónico datospersonales@superbancos.gob.pa .
- Superintendencia de Bancos tendrá un plazo de 2 días hábiles para acusar de recibido a la solicitud.
- Tiempo de respuesta (para solicitar información de sus datos, su eliminación u oponerse a algún tratamiento): menor o igual a 8 días hábiles, a partir de la fecha de solicitud.
- Tiempo de respuesta (para modificar datos errados, inexactos, equívocos o incompletos): 5 días hábiles siguientes a la solicitud de modificación.
- El trámite es gratuito.
- Superintendencia de Bancos entregará información electrónicamente (correo electrónico), si el titular solicita que la información le sea suministrada en USB deberá suministrar este dispositivo al cual será transferida la información o el asumir el costo de esta solicitud. El dispositivo proporcionado por el titular de los datos debe ser suministrado sin formato, ni información.
- Si una vez realizada la solicitud, la Institución no se pronuncia sobre la solicitud del titular de datos personales dentro de los términos establecidos, el titular de los datos personales tendrá derecho a recurrir a la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI).

- El titular tendrá, además, derecho a exigir que se eliminen sus datos personales cuando su almacenamiento carezca de fundamento legal, cuando no hayan sido expresamente autorizados o cuando estuvieran caducos.

En cualquier caso (clientes/proveedores/colaboradores o excolaboradores), si el correo de solicitud llegase incompleto, o no hay claridad de lo que se requiere, en el mismo correo de acuse de recibido, deberá indicarse al titular de los datos la solicitud o lo que deba ser aclarado. El titular de los datos tendrá 5 días hábiles para enviar lo requerido; al día siguiente del vencimiento, de no recibir respuesta o no ser aclarada la misma, se deberá dejar constancia de esto. Una vez el titular de los datos ha aclarado la solicitud a la institución, el tiempo para dar respuesta de diez (10) días hábiles empezará a contar nuevamente.

Formularios para facilitar la información:

- Ejercer el derecho de acceso
- Ejercer el derecho de rectificación
- Ejercer el derecho de cancelación
- Ejercer el derecho de oposición
- Ejercer el derecho de portabilidad

X. Gratuidad del ejercicio de los derechos ARCO:

Todas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de los derechos ARCO serán gratuitas, con las limitaciones que este derecho establece y las que dispongan las leyes especiales en su caso.

XI. Responsable del tratamiento de los datos personales:

Será responsabilidad de la Superintendencia de Bancos con oficinas principales en Av. Samuel Lewis, P.H. Plaza Canaima, planta baja, el tratamiento de los datos personales de clientes, proveedores, titulares de datos gestionados, de colaboradores o excolaboradores, así como la conservación, custodia y buen uso de los datos personales establecidos en cualquier medio provisto que posea la institución. Se ha destinado el correo datospersonales@superbancos.gob.pa, para el ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad.

Son deberes de la Superintendencia de Bancos en materia de protección de datos personales:

- La confidencialidad, respecto a los datos personales objeto de tratamiento a lo que tenga acceso por razón de sus funciones. Para este fin la Superintendencia de Bancos garantizará que las personas autorizadas para tratar los datos personales se comprometan a respetar la confidencialidad, la cual se aplicará durante todo el tiempo que dure el tratamiento y se mantendrá aún cuando hubiese finalizado la relación del colaborador con esta Institución.
- Proporcionar a los titulares de datos personales un instrumento para hacer uso de sus derechos ARCO.

XII. Consulta de la Política de Protección de Datos:

La política, o en su defecto, un extracto de esta, con los aspectos más relevantes del tratamiento realizado a los datos personales y los derechos de los titulares será anunciada, presentada y de fácil acceso desde el sitio web (www.superbancos.gob.pa), así como en las herramientas tecnológicas que manejen datos personales.

La Superintendencia de Bancos garantiza al titular de los datos personales, el ejercicio pleno de sus derechos de acceso, rectificación, cancelación, oposición y portabilidad, a fin de que, con previa acreditación de su identidad, legitimidad y sin costo alguno, tenga acceso a sus derechos.

XIII. Deberes de confidencialidad:

La confidencialidad es uno de los valores institucionales arraigados en la cultura organizacional de la Superintendencia de Bancos; para fortalecer constantemente esto valor que implica guardar reserva de hechos e informaciones de los que se tenga conocimiento con motivo o en ocasión del ejercicio de las funciones laborales, la Superintendencia coordina con la Gerencia de Capacitación, un programa de capacitación y concientización constante en materia de protección de datos personales dentro de la organización, a efectos de promover una cultura de protección de datos en la Institución.

Los responsables del tratamiento de datos personales, los custodios de las bases de datos, así como todas las personas que intervengan en cualquier fase del tratamiento de los datos personales, estarán sujetas al deber de confidencialidad, respecto a los datos que tengan acceso por razón de sus funciones. Lo cual se aplicará durante todo el tiempo que dure el tratamiento y se mantendrá aun cuando hubiese finalizado la relación del colaborador con el responsable del tratamiento o el custodio de la base de datos.

XIV. Datos capturados:

La Superintendencia de Bancos recolecta datos de clientes, proveedores, colaboradores y visitantes.

1. **Clientes:**
   - Información personal.
   - Información laboral.
   - Videovigilancia.

2. **Visitantes:**
   - Información personal.
   - Videovigilancia.

3. **Colaboradores**, se recolectan datos relacionados a:
   - Información personal.
   - Información del dependiente.
   - Información de contacto de emergencia.
   - Información de salud.
   - Datos clínicos (físicos y digitales) para el expediente del colaborador, en la atención de medicina general dentro de la institución.
   - Datos para gestiones de seguro privado.
   - Videos (equipo CCTV)

4. **Proveedores**
   - Información personal como consecuencia de relaciones comerciales.

XV. Tratamiento de los datos personales:

El tratamiento de datos es cualquier operación, complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permita recolectar, almacenar, grabar, organizar, elaborar, seleccionar,

extraer, confrontar, interconectar, asociar, disociar, comunicar, ceder, intercambiar, transferir, transmitir o cancelar datos, o utilizarlos en cualquier otra forma.

La Superintendencia de Bancos realizará el tratamiento (recolección, almacenamiento, uso) de los datos personales, como consecuencia de la funciones o responsabilidades propias ejercidas por la Institución, enmarcados en lo establecido por la ley.

a. Datos de clientes:

Tratamiento	Interés Legítimo
Para brindar contraseñas y acceder a portales que mantiene la Superintendencia como el portal de reclamos, portal de Empleo de Recursos Humanos, Transferencia de Información Digital para los Sujetos Obligados (TIDSO), Campus Virtual	Amparado por consentimiento del titular de los datos
Realizar llamadas o enviar correos a clientes a efectos de notificar resoluciones del proceso de reclamos interpuesto.	Amparado por consentimiento del titular de los datos
Comunicar respuestas a las consultas que se elevan a esta entidad.	Amparado por consentimiento del titular de los datos
Para tramitar las denuncias ante incumplimientos o faltas.	Obligación por mandato regulatorio
Debido a su competencia privativa para conocer y proteger los derechos del consumidor bancario.	Obligación legal

b. Datos de visitantes:

Tratamiento	Interés Legítimo
Para el control de acceso e identificación de las personas que ingresan a las oficinas de la Superintendencia de Bancos, ante posibles incidentes de seguridad. Superintendencia de Bancos comparte edificio con otras empresas, por lo cual no se hace responsable por información requerida en el control de visitantes del edificio donde están las oficinas centrales y en las oficinas que esta mantenga en el interior del país.	Para salvaguardar un interés público
Los videos serán utilizados para el control de seguridad en las instalaciones, de los bienes y servicios de la Institución; y podrán ser utilizados como prueba de cualquier proceso.	Para salvaguardar un interés público

c. Datos de colaboradores: Superintendencia de Bancos realiza tratamientos en cuanto a su rol de empleador.

Tratamiento	Interés Legítimo
Para la vinculación	Para la relación contractual
Desempeño de funciones	
Para Gestión de practicantes	
Para Gestión de formación, con entidades educativas u organismos.	
Para capacitación a entidades financieras	
Para visita de estudiantes	
Para el Desarrollo y formación (becas, capacitaciones, etc.)	
Prestación de servicios, retiro o terminación	
Para dirigir campañas de salud	
Para promoción de colaboradores	
Pagos de salarios	
Afiliaciones y aportes a la Caja del Seguro Social	
Para mantener registro de marcaciones (asistencia) de colaboradores.	
Videos que son utilizados para el control de seguridad en las instalaciones, de los colaboradores, de los bienes y servicios de la Institución; adicional, podrán ser utilizados como prueba de cualquier proceso.	Para salvaguardar un interés público
Fotos en donde aparezcan un colaborador que requiera ser utilizada para alguna publicación, deberá registrarse un consentimiento de la(s) persona(s).	Satisfacer el interés legítimo perseguido por el responsable del tratamiento, prevaleciendo los derechos del titular.
Aportaciones y afiliaciones al Sistema de Ahorro y Capitalización de Pensiones del Servidor Público (SIACAP).	Para la relación contractual
Datos generales y salarios aportados mensualmente a la Contraloría General de la República.	
Informe de planillas y otros que se remiten mensualmente a la Defensoría del Pueblo para su publicación en el Nodo de Transparencia.	
Informe de planillas y otros que se remiten mensualmente a la Autoridad Nacional para la Innovación Gubernamental (ANTAI), para su publicación en sección de “Datos Abiertos”.	
Informe de planillas y otros que se publican en el Nodo de Transparencia de la página Web de la Institución.	
Reportes solicitados por las diferentes Instituciones públicas llámese Contraloría General de la República, Dirección General de Carrera Administrativa (DIGECA), Dirección General de	

Contrataciones Públicas, Órgano Judicial, entre otros.	

d. Datos de proveedores

Tratamiento	Interés Legítimo
Datos personales obtenidos de los participantes, se gestionarán con altos niveles de privacidad y confidencialidad	Para la relación contractual

e. Datos de público en general para la gestión del Recursos Humano y sus hojas de vida

Las hojas de vidas recibidas forman parte del interés del público en general de aplicar a una vacante o de formar parte de una base de datos de profesionales para futuras vacantes del proceso de reclutamiento y selección.

Tratamiento de Datos de público en general, para la gestión del Recursos Humano y sus hojas de vida	Interés Legítimo
De recibir hojas de vida, físicamente, en la recepción de la Institución, o las que lleguen a través de cualquier medio electrónico se harán llegar a la Dirección de Recursos Humanos, quienes evaluarán las mismas y deberán mantener reserva de los datos personales señaladas en estas. Todo colaborador que no pertenezca al área de Planificación y Gestión del Talento, que por alguna circunstancia reciba o tenga acceso a una hoja de vida, deberá eliminarla e indicar a la persona o el interesado, el canal oficial (Portal de empleo) que debe utilizar como parte del proceso de reclutamiento.	• Amparado por consentimiento del titular de los datos (hojas de vida enviadas por medios electrónicos). • Obligación legal (hojas de vidas físicas)

XVI. Plazo de conservación y almacenamiento de los Datos Personales:

Los datos personales serán almacenados de acuerdo con lo establecido por la regulación vigente aplicables a este tipo de documento y hasta por siete (7) años adicionales, salvo que el titular de los datos personales solicitara su eliminación, o autorice menor o mayor tiempo su almacenamiento.

La Superintendencia de Bancos, almacena la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Sin embargo, tal cual lo estipula la Ley, la Superintendencia de Bancos podrá enviar o intercambiar información con autoridades administrativas o judiciales, en ejercicio de sus funciones, cuando se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso con autorización judicial competente.

XVII. Registros de la base de datos

Se deberá mantener registros actualizados de las bases de datos de SBP para realizar los reportes requeridos por la Autoridad de Control.

La Superintendencia de Bancos aplica y se compromete a seguir aplicando las mejores prácticas para garantizar la seguridad de la infraestructura de seguridad informática, la correspondiente protección de datos personales y de las bases de datos que contengan datos personales, garantizando así la confidencialidad, integridad y actualización de los datos gestionados en esta institución.
Se deberá llevar un registro de cada una de las bases de datos con la siguiente información:

- Identificación
- Custodio responsable
- La naturaleza de los datos personales que contiene (descripción del universo de personas que comprende la base de datos)
- Finalidad del tratamiento
- Procedimientos de obtención y tratamiento de los datos
- Destino de los datos y las personas naturales o jurídicas a las que pueden ser transferidos
- Las medidas de seguridad adoptadas, o referencia del documento donde están descritas.
- Los protocolos y la descripción técnica de los datos
- La forma y condiciones en que las personas pueden recibir o acceder a los datos referidos a ellas
- Los procedimientos de obtención y tratamiento de los datos
- El plazo de conservación de los datos
- Cualquier cambio de los elementos indicados

Se deberá mantener un registro actualizado de los tratamientos que se lleven a cabo en la SBP que estarán a disposición de la Autoridad de Control.

XVIII. Seguridad de los datos personales:

En la actualidad, Superintendencia de Bancos cuenta con sistemas estándares de seguridad de datos y comunicaciones encriptado para la transferencia de información. Adicional, se ha agregado una capa externa de murallas de fuego en línea que monitorea el perímetro externo.

La Superintendencia de Bancos está en el proceso de implementar una capa adicional para el control de amenazas de ciberseguridad en tiempo real con detección y acción desatendida apoyado con inteligencia Artificial.

XIX. Procedimiento de gestión de incidentes con datos personales:

Se entiende por incidencia cualquier anomalía que afecte o pudiera afectar la seguridad de las bases de datos o información contenida en las mismas.

En caso de conocer alguna incidencia ocurrida, el usuario debe comunicarla al Oficial de Protección de Datos que adoptará las medidas oportunas frente al incidente reportado.

El Oficial de Protección de Datos Personales informará de la incidencia al Comité de Protección de Datos Personales de esta Superintendencia.

XX. Destrucción

La destrucción de medios físicos y electrónicos se realiza a través de mecanismos que no permiten su reconstrucción. Se realiza únicamente en los casos en que no constituya el desconocimiento de norma legal alguna, dejando siempre la respectiva trazabilidad de la acción.

La destrucción comprende información contenida en poder de terceros como en instalaciones propias.

XXI. Oficial de Protección de Datos:

La Superintendencia de Bancos en su calidad de responsable de los datos personales ha designado un oficial de Protección de Datos (Lourdes De Emiliani, teléfono 506-7979, correo datospersonales@superbancos.gob.pa) o a quien se designe en su reemplazo, quien garantizará la respuesta a los titulares, en los plazos establecidos por la normativa vigente y en la presente política.
Límite de la responsabilidad del oficial de protección de datos: el oficial no será responsable del tratamiento o custodio de la base de datos por prestar sus servicios en la institución.

Las funciones principales del oficial de protección de datos son:

- Servir de canal entre la SBP y el titular de los datos, y asistirles en el ejercicio de sus derechos.
- Garantizar que las respuestas a las solicitudes se proporcionen dentro del tiempo que establece la presente política.
- Informar y asesorar al responsable del tratamiento o custodio de la base de datos, sobre el cumplimiento de la Ley 81 de 2019, de la reglamentación o cualquier disposición legal aplicables en cada caso.
- Supervisar el cumplimiento de la normativa. Para ello podrá examinar, a solicitud del responsable del tratamiento o del custodio de la base de datos o por iniciativa propia, tratamiento de datos personales que se estén llevando a cabo y realizar recomendaciones para la adopción de medidas correctoras necesarias cuando los tratamientos analizados no sean conformes con la normativa aplicable.
- Gestionar con la Gerencia de Capacitación la capacitación constante de las personas que asuman tareas relacionadas con el tratamiento de datos personales.
- Cooperar con la autoridad de control
- Ser la unidad de enlace con la Autoridad de Control.
- Asesorar al responsable del tratamiento o al custodio de la base de datos en la respuesta a los requerimientos u observaciones formalmente notificados por la autoridad de control.
- Coordinar con la Gerencia de Capacitación, un programa de capacitación y concientización constante en materia de protección de datos personales dentro de la organización, a efectos de promover una cultura de protección de datos en la Institución.

XXII. Comité de Protección de Datos:

El Comité de Protección de Datos estará integrado por personal de las áreas que tienen bajo su responsabilidad datos personales, con la finalidad de revisar aquellas solicitudes especiales del titular de los datos y brindar respuesta oportuna a este. De igual forma, el Comité brindará apoyo al Oficial de Datos para el cumplimiento en tiempo de la normativa vigente en materia de protección de datos.

XXIII. Auditorías internas:

Se ejecutarán auditorías al menos una vez al año, en base a la presente política o procedimientos relacionados para:

- Verificar que se cumplan las medidas de seguridad correspondientes a la gestión de datos personales.
- Verificar que se cuente con los registros de consentimientos de los titulares.
- Validar los tiempos de respuesta de las solicitudes presentadas en cumplimiento a la política existente y de la Ley 81 del 2019.
- Entre otros puntos que ayuden detectar o validar que los controles en la gestión de datos personales que realiza la Institución se están realizando de forma correcta.

XXIV. Límites de responsabilidad:

Debido a que las redes sociales constituyen plataformas complementarias de divulgación de información (comunicación) y garantizan elevados niveles de acceso e interconexión con los medios digitales de los usuarios y clientes, no se encuentran bajo responsabilidad de la Superintendencia de Bancos. En consecuencia, cualquier información que los usuarios proporcionen a través de estas plataformas no constituye, ni forma parte de los Datos Personales sujetos a la protección de Superintendencia de Bancos, siendo de total responsabilidad de la persona la información y de las empresas que gestionan estas plataformas.

XXV. Medidas disciplinarias por incumplimiento de la política:

El Comité de Protección de datos comunicará a la Dirección de Recursos Humanos sobre aquellas conductas y/o faltas que no se ajusten a las normas generales señaladas en esta política, con el objetivo de aplicar las medidas disciplinarias correspondientes a los colaboradores.
Las medidas disciplinarias administrativas que se impongan a los colaboradores por incumplir esta política se graduarán según la gravedad de la falta y serán aplicadas en función y concordancia a lo establecido en el Reglamento Interno de la Superintendencia de Bancos.

XXVI. Vigencia

La presente política tendrá vigencia desde la fecha de su emisión o actualización. Nuestra política puede ser revisada o modificada en cualquier momento con el fin de actualizar nuestro compromiso de privacidad para con el titular de los datos personales, en base a las leyes actualizadas sobre privacidad y mejores prácticas.

[F] NOMBRE CASTILLO CHANG AMAURI ARIEL - ID 8-238-386

Firmado digitalmente por [F] NOMBRE CASTILLO CHANG AMAURI ARIEL - ID 8-238-386
Fecha: 2022.10.11 09:45:57 -05'00'

Amauri A. Castillo
Superintendente