POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

CAPÍTULO I: GENERALIDADES

Artículo 1.- Objetivo:

Establecer los lineamientos para la protección de los datos personales que se gestionen en la institución, que incluye el acceso y las decisiones que se tomen alrededor de éstos. El punto central es la protección de los derechos y libertades de los titulares en cuanto al tratamiento de sus datos personales, para dar cumplimiento a la normativa relacionada, especialmente a la Ley Orgánica de Protección de Datos Personales (LOPDP); y a su Reglamento.

Artículo 2.- Alcance:

Las disposiciones de la presente política son de aplicación obligatoria en todo el ámbito de la Corporación Financiera Nacional B.P., al personal y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o convenios con terceros, que tengan relación con la gestión de datos personales.

Los principios y acciones de esta política deben ser reconocidos y de estricto cumplimiento por todo el personal que produce, gestiona, administra y resguarda datos personales en el ejercicio de sus funciones.

La política debe ser concienciada, observada, comunicada y cumplida por todos los servidores, funcionarios, pasantes y colaboradores, sean estos empleados directos, externalizados o servicios profesionales, y por entidades externas como proveedores o entidades de control, los cuales tengan relación con los prestadores de servicios.

El tratamiento de datos personales aplica a la información que se encuentre automatizada o no, así como a toda modalidad de uso posterior. La presente política no se debe aplicar a:

- Personas naturales que utilicen sus datos personales para diferentes actividades familiares o domésticas;
- Personas fallecidas, sin perjuicio de lo que se indica en el artículo 27 de la LOPDP (“Los titulares de derechos sucesorios de las personas fallecidas, podrán dirigirse al responsable del tratamiento de datos personales con el objeto de solicitar el acceso, rectificación y actualización o eliminación de los datos personales del causante, siempre que el titular de los datos no haya, en vida, indicado otra utilización o destino para sus datos”);
- Los datos anonimizados, identificados en el “Inventario de datos personales institucionales”, siempre que no sea posible identificar al titular respectivo;
- Actividades periodísticas y contenidos editoriales;
- Datos personales, cuyo tratamiento se encuentre regulado en normativa especializada de igual o mayor jerarquía en materia de gestión de riesgos por desastres naturales; y, seguridad y defensa del Estado;
- Bases de datos establecidas, para la prevención, investigación, detección o enjuiciamiento de infracciones penales o relacionadas con procesos judiciales realizado por los organismos estatales competentes en cumplimiento de sus funciones legales;
- Datos que identifican o hacen identificables a personas jurídicas.

En lo que se refiere a la aplicación territorial, se debe considerar:

- La institución realizará el tratamiento de los datos personales, de acuerdo a lo establecido en el Inventario de datos personales institucionales, en las instalaciones de la Corporación Financiera Nacional B.P. y de identificarse alguna excepción, será especificada puntualmente en el A-GCI-PDP-03 De Privacidad de la Información y Protección de Datos, de tal manera que el titular tenga el conocimiento respectivo.
- El responsable o encargado del tratamiento de datos personales en la institución se encuentre domiciliado en el país.

Artículo 3.- Base Legal/Normativa CFN B.P.

3.1. Base Legal

3.1.1. Constitución de la República del Ecuador, Registro Oficial No 449 del 20 de octubre de 2008.
3.1.2. Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos, Ley No 67 publicada en el Registro Oficial Suplemento No 557 del 17 de abril de 2002.
3.1.3. Código Orgánico Monetario y Financiero,Libro I publicado en el Registro Oficial No 332 del 12 de septiembre de 2014.
3.1.4. Ley Orgánica de Protección de Datos Personales, publicada en el Registro Oficial Suplemento No. 459 del 26 de mayo de 2021.
3.1.5. Reglamento General de la Ley Orgánica de Protección de Datos Personales, publicado en el Tercer Suplemento del Registro Oficial No. 435 el 13 de noviembre de 2023.
3.1.6. Resoluciones emitidas por la Superintendencia de Protección de Datos.
3.1.7. Codificación de las Normas de la Superintendencia de Bancos, Título IX de la Gestión y Administración de Riesgos, Capítulo V Norma de Control para la Gestión del Riesgo Operativo,
3.1.8. Ley Orgánica de Transparencia y Acceso a la Información Pública, publicada en el Registro Oficial, suplemento nro. 245, de fecha 7 de febrero de 2023.
3.1.9. NORMA ISO/IEC 27001 Sistemas de Gestión de Seguridad de la Información Requerimientos.
3.1.10. NORMA ISO/IEC 17799:2005 – 27002 Tecnología de la información - Técnicas de seguridad - Código de práctica para la gestión de seguridad de la información.
3.1.11. INEN ISO/IEC 27005 Gestión del Riesgo en la Seguridad de la Información.
3.1.12. EGSI–Esquema Gubernamental de Seguridad de la Información. EGSI, Mecanismo para Implementar el Sistema de Gestión de Seguridad de la Información en el Sector Público. Acuerdo No- MINTEL-MINTEL-2024-0003 publicado en el Tercer Suplemento del Registro Oficial No. 509 del 01 de marzo de 2024 Normativa institucional CFN B.P.

3.2. Normativa de la Corporación Financiera Nacional B.P.

3.2.1 Libro I: Operaciones Financieras, Título V: Lavado de Activos: Subtítulo I: Prevención de Lavado de Activos:
3.2.1.1. Capítulo I: Manual de Administración del Riesgo de Lavado de Activos y Financiamiento de Delitos, como el Terrorismo (ARLAFDT).
3.2.1.2. Capítulo II: Manual del Sistema de Prevención y Administración de Riesgo de Lavado de Activos, Financiamiento del Terrorismo y Otros Delitos (SPARLAFTD).
3.2.2 Libro II: Normativa sobre Administración; Título IV Recursos Humanos; Subtítulo III Código de Ética de la Corporación Financiera Nacional B.P.

3.2.2.1. Libro II: Normativa sobre Administración; Título XVII Seguridad de la Información; Subtítulo I: Políticas Institucionales para el Sistema de Gestión de Seguridad de la Información.

Artículo 4.- Responsabilidad del Tratamiento

De acuerdo con la Ley Orgánica de Protección de Datos Personales el responsable del tratamiento de datos personales es la Corporación Financiera Nacional B.P. como persona jurídica.

Los comités, delegados, propietarios de procesos y servidores cumplen funciones técnicas u operativas; sin embargo, la responsabilidad final por el tratamiento recae en la institución

Artículo 5.- Glosario de Términos:

5.1. Autoridad de protección de datos personales.- Autoridad pública independiente encargada de supervisar la aplicación de la LOPDP, su respectivo reglamento y las resoluciones que emita, con el fin de proteger los derechos y libertades fundamentales de las personas naturales, en cuanto al tratamiento de sus datos personales.
5.2. Anonimización.- Es un proceso que convierte los datos, de tal manera que no se pueda identificar a los individuos.
5.3. Base de Datos o ficheros.- Es un conjunto de datos relacionados y estructurados, ordenados de modo sistemático para su posterior recuperación, análisis y/o transmisión.
5.4. CASI.- Comité de Administración de Seguridad de la Información, órgano colegiado encargadode conocer, evaluar y aprobar iniciativas, lineamientos, procedimientos, instrumentos y reportes en materia de seguridad de la información, ciberseguridad y protección de datos personales, segun sus funciones establecidas en el Reglamento del CASI y demás normativa aplicable Su rol es de gobernanza y supervisión, sin perjuicio de que la responsabilidad del tratamiento de datos recae en la CFN B.P., conforme a la LOPDP.
5.5. Confidencialidad de los datos.- Garantizar que los datos sean accesibles sólo a aquellas personas autorizadas a tener acceso a la misma.
5.6. Consentimiento.- Manifestación de la voluntad libre, específica, informada e inequívoca, por el que el titular de los datos personales autoriza al responsable del tratamiento de los datos personales a tratar los mismos para fines específicos.
5.7. Dato biométrico.- Dato personal, relativo a las características únicas de los seres humanos, sean físicas o fisiológicas, o conductas de una persona natural que permita o confirme su identificación. Por ejemplo imágenes faciales o datos dactiloscópicos, entre otros.
5.8. Dato genético.- Dato personal único, que diferencia a los individuos entre sí, relacionado a características genéticas heredadas o adquiridas de una persona natural que proporcionan información única sobre la fisiología o salud de un individuo.
5.9. Dato personal.- Dato que identifica o hace identificable a una persona natural, directa o indirectamente.
5.10. Datos personales crediticios.- Datos que integran el comportamiento económico de personas naturales, para analizar su capacidad financiera.
5.11. Datos relativos a la salud.- Datos personales relativos a la salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.
5.12. Datos sensibles.- Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.

5.13. Delegado de protección de datos personales.- Persona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la autoridad de protección de datos personales, sirviendo como punto de contacto entre esta y la entidad responsable del tratamiento de datos. Esta delegación debe ser realizada de manera formal por el/la Gerente General.

5.14. Destinatario.- Persona natural o jurídica que ha sido comunicada con datos personales.

5.15. Disponibilidad de los datos.- Garantizar que los usuarios autorizados tengan acceso a los datos y a los recursos relacionados con los mismos, siempre que lo requieran.

5.16. Elaboración de perfiles.- Todo tratamiento de datos personales que permite evaluar, analizar o predecir aspectos de una persona natural para determinar comportamientos o estándares relativos a: rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, ubicación, movimiento físico de una persona, entre otros.

5.17. Encargado del tratamiento de datos personales.- Persona natural o jurídica, pública o privada, autoridad pública, u otro organismo que solo o conjuntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales.

5.18. Entidad Certificadora.- Entidad reconocida por la autoridad de protección de datos personales, que podrá, de manera no exclusiva, proporcionar certificaciones en materia de protección de datos personales.

5.19. Fuente accesible al público.- Bases de datos que pueden ser consultadas por cualquier persona, cuyo acceso es público, incondicional y generalizado.

5.20. Integridad de los Datos.- Salvaguardar la totalidad y exactitud de los datos, así como, los métodos de procesamiento.

5.21. LOPDP.- Ley orgánica de protección de datos personales.

5.22. PAC.- Plan Anual de Contrataciones.

5.23. POA.- Plan Operativo Anual.

5.24. Responsable de tratamiento de datos personales.- Persona natural o jurídica, pública o privada, autoridad pública, u otro organismo, que solo o conjuntamente con otros decide sobre la finalidad y el tratamiento de datos personales. En el caso de la CFN B.P., el responsable del tratamiento es la persona jurídica en su conjunto, no un órgano, comité o funcionario en particular.

5.25. Sellos de protección de datos personales.- Acreditación que otorga la entidad certificadora al responsable o al encargado del tratamiento de datos personales, de haber implementado mejores prácticas en sus procesos, con el objetivo de promover la confianza del titular, de conformidad con la normativa técnica emitida por la autoridad de protección de datos personales.

5.26. Seudonimización.- Tratamiento de datos personales de manera tal que ya no puedan atribuirse a un titular sin utilizar información adicional, siempre que dicha información adicional, figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

5.27. Titular.- Persona natural cuyos datos son objeto de tratamiento.

5.28. Transferencia o comunicación.- Manifestación, declaración, entrega, consulta, interconexión, cesión, transmisión, difusión, divulgación o cualquier forma de revelación de datos personales realizada a una persona distinta al titular, responsable o encargado del tratamiento de datos personales. Los datos personales que comuniquen deben ser exactos, completos y actualizados.

5.29. Tratamiento.- Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación,

indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales.

5.30. Volumen de Negocio.- A efectos del régimen sancionatorio, se entiende por volumen de negocio, a la cuantía resultante de la venta de productos y de la prestación de servicios realizados por operadores económicos, durante el último ejercicio que corresponda a sus actividades, previa deducción del Impuesto al Valor Agregado y de otros impuestos directamente relacionados con la operación económica.

5.31. Vulneración de la seguridad de los datos personales.- Incidente de seguridad que afecta la confidencialidad, disponibilidad o integridad de los datos personales.

Artículo 6.- Tratamiento Legítimo de Datos Personales

Se entenderá que el tratamiento de datos personales es legítimo, si se cumple con alguna de las siguientes características:

- Si se cuenta con el consentimiento explícito del titular, para un asunto en particular o para varias finalidades específicas.
- Si es realizado por el responsable de tratamiento de datos personales, en cumplimiento de una obligación legal o por orden judicial.
- Si es realizado por el responsable de tratamiento de datos personales, para sustentar el cumplimiento de una misión de interés público, o para dar cumplimiento a una normativa.
- A petición del titular para la ejecución de medidas precontractuales o para la ejecución de medidas contractuales perseguidas por el responsable, encargado o por un tercero legalmente habilitado.
- Para proteger la vida, salud, integridad y en general para proteger intereses vitales, ya sea del titular o de otra persona natural, que esté relacionada con los procesos institucionales.
- Si se realiza el tratamiento de datos personales que consten en bases de datos de acceso público.
- En el caso que se necesite satisfacer un interés legítimo del responsable del tratamiento de datos o de un tercero, siempre que no prevalezca el interés o lo derechos fundamentales que tienen los titularos al amparo de la normativa vigente, especialmente de la Ley Orgánica de Protección de Datos Personales, su Reglamento y resoluciones que emita la Superintendencia de Protección de Datos Personales.

Artículo 7.- Consentimiento del Tratamiento de Datos Personales

Se entiende como la manifestación de la voluntad del titular para que se dé tratamiento y comunicación de sus datos personales y se considera válido si:

- Es libre, sin presiones de ningún tipo y esté exenta de vicios.
- Es específica, es decir, detallada de manera concreta, sobre los medios y fines del tratamiento que se le dará a sus datos personales.
- Es informada al titular, para que se dé cumplimiento a los principios de transparencia y se garantice el derecho a la transparencia.
- Es inequívoca, es decir que no haya confusión o dudas sobre el alcance de la autorización por parte del titular.

Es importante mencionar que el consentimiento puede revocarse (proceso lícito porque no tiene efectos retroactivos), de la misma manera que se gestionó el consentimiento, sin que sea necesario presentar una justificación.

Un consentimiento puede abarcar una pluralidad de finalidades, pero es importante que se detalle claramente en el consentimiento del titular, el alcance de la misma.

Artículo 8.- Interés Legítimo

Se considera que el tratamiento de datos personales tiene interés legítimo cuando:

- Se traten únicamente los datos personales, que sean necesarios para cumplir los procesos institucionales.
- El responsable del tratamiento de los datos personales garantice al titular el manejo adecuado y transparente de su información.

La autoridad de protección de los datos personales, tiene la potestad de requerir al responsable, un informe de los riesgos asociados a los datos personales, que le permita identificar las amenazas o vulnerabilidades, para garantizar los derechos fundamentales a los titulares de acuerdo a las normativas vigentes.

Artículo 9.- Principios

a) Juridicidad.- Dar cumplimiento a la normativa relacionada con la protección de datos personales y garantizar los derechos de sus titulares.
b) Transparencia.- La institución garantiza un adecuado tratamiento de los datos personales de acuerdo a las normativas vigentes y velando por el cumplimiento de los derechos de sus titulares.
c) Confidencialidad.- Garantizar que los datos personales van a estar disponibles únicamente a las personas que tengan expresamente el consentimiento para su acceso y para el tratamiento correspondiente.
d) Calidad y exactitud.- Es responsabilidad de los propietarios de la información garantizar la calidad y exactitud de los datos personales, de tal manera de velar por su integridad.
e) Conservación.- Los datos personales estarán disponibles en función al A-GCI-PDP-03 De Privacidad de la Información y Protección de Datos , en concordancia con lo establecido en los procesos institucionales.
f) Seguridad de datos personales.- A los datos personales se les aplicará las seguridades establecidas en las políticas institucionales de seguridad de la información.
g) Interdisciplinariedad.- Las normativas internas, relacionadas con la protección de datos personales, que se generen en la institución, deben ser revisadas previamente por las unidades administrativas que participen en el tratamiento de datos personales.

Artículo 10.- Niveles de Revisión y Aprobación:

El Comité de Administración de la Seguridad de la Información, entre sus atribuciones y responsabilidades consta la de ejercer el nivel de revisión y gestionar la aprobación de las normas institucionales en materia de seguridad de la información ante el Directorio de la institución.

Considerando las funciones y responsabilidades actuales que el Comité de Administración de la Seguridad de la Información mantiene, le corresponde, aprobar el “Informe de verificación y evaluación de seguridad de datos personales” que permitirá hacer un seguimiento del cumplimiento

a la presente política. Estas acciones se enmarcan en su rol de supervisión y gobernanza, sin que ello implique la asunción de la responsabilidad del tratamiento de datos personales, la cual corresponde exclusivamente a la CFN B.P. como persona jurídica.

Artículo 11.- Prevención de Lavado de Activos

Es responsabilidad de todos los funcionarios que participan en los distintos procesos de protección de datos personales aplicar y dar cumplimiento a las medidas de seguridad para el mantenimiento de la información recabada para la aplicación de la debida diligencia prevista en el "Manual de administración del riesgo de lavado de activos y financiamiento de delitos, como el terrorismo" (ARLAFDT); o en el "Manual del sistema de prevención y administración de riesgo de lavado de activos, financiamiento del terrorismo y otros delitos" (SPARLAFTD).

CAPÍTULO II: DERECHOS RELACIONADOS CON LA PROTECCIÓN DE DATOS PERSONALES

Artículo 12.- Derechos:

La CFN B.P. garantiza que sus clientes, servidores, funcionarios, o personal externo con alguna vinculación a la institución, usuarios, colaboradores, proveedores, accionistas, aliados y en general de todos sus grupos de interés respecto de los cuales la institución ejerce el tratamiento de la información personal (el término cliente también incluye a aquellos individuos cuya relación comercial ha terminado, pero cuya información o datos personales se conserven), puedan ejercer derechos respecto a la Ley Orgánica y de Protección de Datos Personales y beneficiarse de servicios de la más alta calidad. El titular de los datos personales, en cualquier momento, puede hacer una solicitud formal (mediante memorando,oficio o mediante el correo pdp@cfn.fin.ec según sea el caso), dirigido al delegado de protección de datos personales.

Sin perjuicio de lo dispuesto en la LOPDP, los derechos que le asisten son:

Derecho a la información.- En el momento de la recolección o antes de recopilar datos personales para cualquier tipo de actividades de tratamiento, incluidas, entre otras, la prestación de servicios o actividades comerciales, CFN B.P. es responsable de informar adecuadamente a los titulares sobre los siguientes tipos de datos personales: los tipos de datos personales recolectados, los fines del tratamiento, los métodos de tratamiento, los derechos de los titulares con respecto a sus datos personales, el período de conservación, las posibles transferencias de datos internacionales, si los datos serán compartidos con terceros y las medidas de seguridad de CFN B.P. para proteger los datos personales.

Cuando los datos personales no se obtuvieren de forma directa del titular o fueren obtenidos de una fuente accesible al público, será responsabilidad del encargado o responsable de protección de datos personales, informar al titular dentro de los siguientes treinta (30) días o al momento de la primera comunicación con el titular, cualquiera de las dos circunstancias que ocurra primero.

Derecho de acceso.- El titular tendrá derecho a conocer y obtener gratuitamente acceso a todos sus datos personales. El responsable del tratamiento de datos personales atenderá las solicitudes dentro del plazo de quince (15) días.

Derecho de rectificación y actualización.- El titular tiene el derecho a obtener del responsable del tratamiento la rectificación y actualización de sus datos personales inexactos o incompletos siempre que presente los justificativos del caso. El responsable del tratamiento de datos personales atenderá las solicitudes dentro del plazo de quince (15) días.

Derecho de eliminación.- El titular tiene derecho a obtener la supresión de los datos personales que le conciernan cuando:

1) El tratamiento no cumpla con los principios de esta política o de la normativa relacionada con la protección de datos personales;
2) El tratamiento no sea necesario o pertinente para el cumplimiento de la finalidad a la que se dio consentimiento;
3) Los datos personales hayan cumplido con la finalidad para la cual fueron recogidos o tratados;
4) Haya vencido el plazo de conservación de los datos personales;
5) El tratamiento afecte derechos fundamentales o libertades individuales;
6) Revoque el consentimiento prestado o señale no haberlo otorgado para uno o varios fines específicos, sin necesidad de que medie justificación alguna; o,
7) Exista obligación legal.

El responsable del tratamiento de datos personales atenderá las solicitudes dentro del plazo de quince (15) días.

Derecho de oposición.- El titular tiene el derecho a oponerse o negarse al tratamiento de sus datos personales, en los siguientes casos:

1) No se afecten derechos y libertades fundamentales de terceros, la ley se lo permita y no se trate de información pública, de interés público o cuyo tratamiento está ordenado por la normativa de protección de datos personales.
2) El tratamiento de datos personales tenga por objeto la mercadotecnia directa; el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles; en cuyo caso los datos personales dejarán de ser tratados para dichos fines.
3) Cuando no sea necesario su consentimiento para el tratamiento como consecuencia de la concurrencia de un interés legítimo, previsto en el artículo 7 de la presente política, y se justifique en una situación concreta personal del titular, siempre que una ley no disponga lo contrario.

El responsable del tratamiento dejará de tratar los datos, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones. La solicitud del titular será atendida dentro del plazo de quince (15) días.

Derecho a la portabilidad.- Los titulares de los datos tienen derecho a recibir, previa solicitud, una copia de los datos que nos proporcionaron en un formato estructurado y a transmitir esos datos a otro responsable, cuando sea técnicamente posible, y siempre que se cumpla con alguno de los siguientes enunciados:

1) Que el titular haya otorgado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. La transferencia o comunicación se hará entre responsables del tratamiento de datos personales cuando la operación sea técnicamente posible; en caso contrario los datos serán transmitidos directamente al titular.
2) Que el tratamiento se efectúe por medios automatizados;
3) Que se trate de un volumen relevante de datos personales, según los parámetros definidos en el reglamento de la presente ley; o,
4) Que el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos del responsable o encargado del tratamiento de datos personales, o del titular en el ámbito del derecho laboral y seguridad social.

No procederá este derecho cuando se trate de información obtenida a partir del tratamiento con base en los datos personales proporcionados por el titular.

Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad

Serán excepciones en los siguientes casos:

a) Si el solicitante no es el titular de los datos personales o su representante legal no se encuentre debidamente acreditado.
b) Cuando los datos son necesarios para el cumplimiento de una obligación legal o contractual.
c) Cuando los datos son necesarios para el cumplimiento de una orden judicial, resolución o mandato motivado de autoridad pública competente.
d) Cuando los datos son necesarios para la formulación, ejercicio o defensa de reclamos o recursos.
e) Cuando se pueda causar perjuicios a derechos o afectación a intereses legítimos de terceros y ello sea acreditado por el responsable de la base de datos al momento de dar respuesta al titular a su solicitud de ejercicio del derecho respectivo.
f) Cuando se pueda obstaculizar actuaciones judiciales o administrativas en curso, debidamente notificadas.
g) Cuando los datos son necesarios para ejercer el derecho a la libertad de expresión y opinión.
h) Cuando los datos son necesarios para proteger el interés vital del titular o de otra persona natural.
i) En los casos en los que medie el interés público, sujeto al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de la LOPDP, la presente política y a los criterios de legalidad, proporcionalidad y necesidad.
j) En el tratamiento de datos personales que sean necesarios para el archivo de información que constituya patrimonio del Estado, investigación científica, histórica o estadística.

Derecho a la suspensión del tratamiento.- El titular tendrá derecho a obtener del responsable del tratamiento la suspensión del tratamiento de los datos, cuando se cumpla alguna de las condiciones siguientes:

Condición	Consideraciones
El titular impugna exactitud de datos personales.	De existir negativa por parte del responsable o encargado del tratamiento de datos personales, y el titular recurra por dicha decisión ante la autoridad de protección de datos personales, esta suspensión se extenderá hasta la resolución del procedimiento administrativo. Cuando el titular impugne la exactitud de los datos personales, mientras el responsable de tratamiento verifica la exactitud de los mismos, deberá colocarse en la base de datos, en donde conste la información impugnada, que ésta ha sido objeto de inconformidad por parte del titular.
El tratamiento es ilícito y el titular se oponga a la supresión de datos personales y solicite la limitación de uso.	
El responsable ya no necesite los datos personales para los fines del tratamiento, pero el titular los necesite para la formulación, el ejercicio o la defensa de reclamaciones.	
Cuando el titular se haya opuesto al tratamiento, conforme se establece en el artículo 15 de la presente política, respecto al tratamiento de datos relativos a la salud.	

Derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas.- El titular tiene derecho a no ser sometido a una decisión basada única o parcialmente en valoraciones que sean producto de procesos automatizados, incluida la elaboración

de perfiles, que produzcan efectos jurídicos en él o que atenten contra sus derechos y libertades fundamentales, para lo cual se dispondrán de los procedimientos de atención y resolución de solicitudes, no aplicará este derecho cuando la decisión está asociada a la provisión del servicio o por orden judicial.

Derecho de consulta.- Las personas tienen derecho a la consulta pública y gratuita ante el Registro Nacional de Protección de Datos Personales.

CAPÍTULO III: TRATAMIENTO DE DATOS PERSONALES

Artículo 13.- Consideraciones para el Tratamiento de Datos Personales

El responsable del tratamiento de datos personales, coordinará con los propietarios de la información, la generación del Inventario de datos personales institucionales que se identifiquen en los cuales se dé tratamiento de datos personales, de tal manera de identificar datos genéricos por cada categoría identificada, que permita hacer un análisis de los riesgos, así como también de amenazas y oportunidades.

Una vez que se tenga actualizado el "Inventario de datos personales institucionales" de la categoría identificada con el propietario de la información, se debe hacer el análisis de riesgos de datos personales, siguiendo el "Manual de Procedimientos para el Control y Mitigación de Riesgos de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales", hasta llegar a tener la matriz de riesgos actualizada (identificando aquellos riesgos relacionados con la protección de datos personales y con su respectiva categoría), en la cual consten los riesgos cuyo riesgo neto o residual tenga una calificación menor a "3", porque sobre ellos se debe plantear los respectivos planes de acción.

Como parte del análisis de riesgos, también se deben analizar las amenazas y oportunidades para cada proceso institucional identificado por el propietario de la información, que resultará fundamental cuando se realice el "Informe de verificación y evaluación de seguridad de datos personales".

Mediante el "Informe de verificación y evaluación de seguridad de datos personales", se pueden plantear cambios, actualizaciones o mejoras, al Inventario de datos personales institucionales, los cuales deben ser conocidos por todos los integrantes del "Sistema de protección de datos personales" y debe ser documentado como parte del proceso de mejora continua. El Registro nacional de protección de datos personales institucional se basa en el Inventario de datos personales institucionales; de ahí la importancia de mantenerlo actualizado de manera permanente y debe ser actualizado por cada instancia generada del proceso institucional correspondiente.

Artículo 14.- Categorías especiales de Datos Personales

De acuerdo a la LOPDP, las categorías especiales de datos personales son:

a) Datos sensibles;
b) Datos de niñas, niños y adolescentes;
c) Datos de salud; y
d) Datos de personas con discapacidad y de sus sustitutos, relativos a la discapacidad.

Artículo 15.- Tratamiento de datos Personales en CFN.B.P.

Todos los clientes, servidores, funcionarios, o personal externo con alguna vinculación a la institución, usuarios, colaboradores, proveedores, accionistas, aliados y en general de todos sus grupos de interés respecto de los cuales la institución ejerce el tratamiento de la información personal (el término cliente también incluye a aquellos individuos cuya relación comercial ha terminado, pero cuya información o datos personales se conserven), que realicen tratamiento de datos sensibles, ya sean digitalizados o en documentos físicos, deben firmar el acuerdo de confidencialidad de acuerdo a las “Políticas institucionales para el sistema de gestión de seguridad de la información”.

El tratamiento de los datos personales sensibles únicamente se podrá realizar cuando el titular haya dado su consentimiento explícito mediante el A-GCI-PDP-03 De Privacidad de la Información y Protección de Datos, o que por una instancia legal hayan sido requeridos y estén especificados claramente los fines para los cuales se utilizarán estos datos.

La institución debe comunicar a sus clientes, servidores, funcionarios, o personal externo con alguna vinculación a la institución, usuarios, colaboradores, proveedores, accionistas, aliados y en general de todos sus grupos de interés respecto de los cuales la institución ejerce el tratamiento de la información personal (el término cliente también incluye a aquellos individuos cuya relación comercial ha terminado, pero cuya información o datos personales se conserven), mediante notificaciones o ventanas emergentes en las páginas web, información sobre la política de privacidad y el tratamiento de sus datos.

Toda comunicación a los clientes, servidores, funcionarios y personal externo, sobre la política de privacidad y del tratamiento de sus datos, debe incluir siempre un texto que indique su aceptación expresa.

Todo acceso concedido a un tercero a los datos personales sobre los cuales se realiza su tratamiento institucional, estará restringido al propósito de negocio entre la institución y la tercera entidad. El titular debe tener conocimiento de esta situación.

Toda la información de datos personales sensibles, que se proporcione a la institución, como por ejemplo, dirección, correo electrónico, números de celular y cualquier otro dato que lo identifique como parte del tratamiento de datos institucional, no será revelada a terceros mientras no operen bajo una relación contractual con la Corporación Financiera Nacional B.P. y se cuente con la autorización del titular.

Cuando el titular no está capacitado, física o jurídicamente para dar su consentimiento para el tratamiento de sus datos, se podrá realizar por medio de la aprobación de su representante legal.

Se podrá hacer el tratamiento de los datos personales cuando se cuente con la autorización expresa del titular o cuando se realiza por una orden de autoridad judicial.

Se podrá hacer el tratamiento de los datos personales cuando sea por fines de interés público, fines de investigación científica o histórica o fines estadísticos, siempre protegiendo los intereses y derechos del titular.

Como parte del levantamiento del “Inventario de datos personales institucionales”, la Gerencia de Administración del Talento Humano, a través del Departamento Médico debe identificar los datos de salud del personal de la institución a los cuales se realizará el tratamiento respectivo, siempre que se sujeten a las disposiciones contenidas en la LOPDP.

Todos los servidores y funcionarios de CFN B.P., cuando realicen el tratamiento de los datos personales, deben garantizar el derecho a la intimidad personal, familiar, respetando la vida privada de las personas.

El titular de datos personales, en cualquier momento podrá hacer solicitudes relacionadas con el tratamiento de sus datos personales (requerimientos, peticiones, quejas, reclamos, etc., de manera formal, mediante memorando u oficio según sea el caso, dirigidas al delegado de protección de datos personales de la institución, quien de manera coordinada con el encargado y el responsable gestionará los requerimientos.

La institución debe informar la "Política Institucional para el sistema de gestión de protección de datos personales", en cada canal electrónico que disponga para comunicarse con el ciudadano.

Mediante el A-GCI-PDP-03 De Privacidad de la Información y Protección de Datos, la institución entregará la información suficiente al titular, relacionada con el tratamiento de datos personales, que le permita conocer la finalidad a que se destinarán sus datos y el tipo de actividad del tercero a quien se pretende transferir o comunicar sus datos.

Los requerimientos de acceso, rectificación, actualización o eliminación de los datos personales serán atendidos por el responsable del tratamiento de datos personales de la CFN B.P.:

a) De titulares,
b) De titulares de derechos sucesorios de las personas fallecidas,
c) Del representante legal de menores de edad o personas incapaces reconocidas por la ley.

Los datos personales crediticios a los cuales se les dará tratamiento en la institución, deben ser comunicados al titular, mediante el A-GCI-PDP-03 De Privacidad de la Información y Protección de Datos.

La institución podrá realizar el tratamiento de datos personales crediticios de carácter financiero, bancario o comercial obtenidos de fuentes de acceso público o procedente de información facilitadas por el acreedor, siempre que sean utilizados solamente para finalidad de análisis y no sean comunicados o difundidos.

Los datos crediticios no podrán tener otra finalidad secundaria y en ningún caso podrán comunicarse una vez transcurridos cinco años desde que la obligación a la que se refieren se haya hecho exigible.

Cumplidos los plazos establecidos en el A-GCI-PDP-03 De Privacidad de la Información y Protección de Datos, los datos personales deben ser destruidos o devueltos al responsable del tratamiento de datos personales bajo la supervisión de la autoridad de protección de datos personales.

La institución tiene la obligación de contestar las solicitudes de información del titular en un término de 15 días, ya sea para admitirla o rechazarla de forma justificada.

El titular puede solicitar al prestador de información de sus referencias crediticias, que durante el plazo de elaboración de la información solicitada, señalen en los reportes de crédito que emitan, que la información materia de la solicitud está siendo revisada a pedido del titular.

En el caso que la institución identifique la necesidad de implementar una herramienta tecnológica para una mejor administración de los datos personales, la Gerencia de Seguridad de la Información

será responsable de definir los proyectos que se requieran, los lineamientos y gestionar las acciones necesarias (incluyendo asignaciones presupuestarias, aprobaciones, POA, PAC, etc.), la cual será implementada en la institución, con la participación de la Gerencia de Innovación Tecnológica.
El titular puede revocar en cualquier momento y sin justificación alguna la autorización de transferencia de datos personales a un tercero.

Los destinatarios de los datos también deben cumplir con esta política y con la normativa relacionada con la protección de datos personales.

Todos los datos de carácter personal, tales como ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás relativos a la intimidad personal y en especial aquella información, cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales son confidenciales de acuerdo a la ley LOPDP.

Los profesionales de la salud de la CFN B.P. pueden recolectar y tratar los datos relativos a la salud de sus pacientes, que estén o hubiesen estado bajo tratamiento, de acuerdo a lo previsto en la presente política, en la LOPDP o en la legislación especializada sobre la materia y demás normativa dictada por la autoridad de protección de datos personales en coordinación con la autoridad sanitaria nacional siempre con la respectiva aprobación del titular.

Los profesionales de la salud de la institución que recolecten y traten los datos de salud de sus pacientes, tienen el deber de garantizar la confidencialidad de los datos, implementando medidas técnicas y organizativas apropiadas para prevenir la pérdida, tratamiento ilícito, destrucción o daño accidental mediante técnicas adecuadas.

No se requerirá el consentimiento del titular cuando el tratamiento sea por razones de interés público en el ámbito de la salud pública.

Los datos de salud constituyen datos personales sensibles y deberán ser tratados con medidas técnicas y organizativas reforzadas que garanticen su confidencialidad, integridad y disponibilidad. Siempre que sea posible y compatible con la finalidad del tratamiento, se aplicarán técnicas de anonimización o seudonimización para reducir los riesgos de identificación de los titulares
Todo tratamiento de datos de salud anonimizados será autorizado previamente por la autoridad de protección de datos personales, previa presentación del protocolo técnico que garantice la protección de dichos datos y el informe previo favorable emitido por la autoridad sanitaria.

No es necesaria la autorización del titular cuando el tratamiento sea para proteger intereses vitales del propio titular, el titular no esté capacitado, física o jurídicamente, para dar su consentimiento; o sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social.

Los datos personales podrán transferirse o comunicarse a terceros cuando tenga el consentimiento del titular y sea con fines directamente relacionados con las funciones legítimas del responsable y del destinatario.

Todo tratamiento de datos personales realizado por el encargado o por terceros, debe estar establecido en el A-GCI-PDP-03 De Privacidad de la Información y Protección de Datos, en el que se establezca de manera clara y precisa, que el tratamiento de los mismos se hará conforme las instrucciones del responsable y que no los utilizará para finalidades diferentes a las señaladas.

El encargado, será responsable de las infracciones derivadas del incumplimiento de las condiciones de tratamiento de datos personales establecidas en la presente política y en la normativa relacionada con la protección de datos personales.

Sin perjuicio de las funciones asignadas a los servidores, delegados y al CASI, la responsabilidad del tratamiento de datos personales, recae íntegramente en la CFN B.P., conforme a lo establecido por la LOPDP y ratificado por la Autoridad de Protección de Datos personales.

Eliminación de los Datos Personales

Una vez cumplido el período de vigencia del tratamiento de datos personales, de acuerdo a lo establecido en el A-GCI-PDP-04 Inventario de datos personales institucionales, el encargado del tratamiento de datos personales, procederá a la eliminación respectiva, con base al A-GCI-PDP-03 De Privacidad de la Información y Protección de Datos; además debe registrar esta acción en el A-GCI-PDP-05 Bitácora de eliminación de datos personales, de tal manera de dejar su constancia.

CAPÍTULO IV: TRANSFERENCIA O COMUNICACIÓN DE DATOS PERSONALES A TERCEROS

Artículo 16.- Transferencias de Datos Personales

No es necesaria la autorización del titular para la transferencia de los datos personales cuando son obtenidos en fuentes públicas, por relaciones jurídicas entre el responsable y el titular, cuando los datos sean para autoridades administrativas o judiciales, para Administraciones públicas con fines históricos, estadísticos o científicos, cuando los datos de salud solucionen una urgencia de los intereses vitales del titular o sirvan para estudios epidemiológicos, siempre que estén anonimizados.

El encargado o responsable podrá transferir los datos personales o comunicarse a terceros, siempre que se lo realice para su tratamiento respectivo, de acuerdo al "Inventario de datos personales institucionales" y al consentimiento del titular.

CAPÍTULO V: TRANSFERENCIA O COMUNICACIÓN INTERNACIONAL DE DATOS PERSONALES

Artículo 17.- Transferencia Internacional de Datos Personales

Se podrán transferir o comunicar datos personales a países, organizaciones y personas jurídicas en general, que brinden niveles adecuados de protección y que se ajusten a estándares internacionales y que estén conforme a los criterios establecidos en el Reglamento a la Ley Orgánica de Protección de Datos Personales.

Para las transferencias internacionales de datos a un país, organización o territorio económico internacional que no haya sido calificado por la autoridad de protección de datos personales, de tener un nivel adecuado de protección, se puede realizar la transferencia siempre que el responsable o encargado del tratamiento de datos personales ofrezca garantías adecuadas para el titular, siempre que cumpla lo siguiente:

1. Garantizar el cumplimiento de principios, derechos y obligaciones en un estándar igual o mayor a la normativa.

2. Disponibilidad permanente de acciones administrativas o judiciales respecto a la protección de datos personales.
3. Derecho a solicitar reparación integral de ser el caso.

Los responsables o encargados del tratamiento de datos personales podrán presentar a la autoridad de protección de datos personales, normas corporativas vinculantes, específicas y aplicadas al ámbito de su actividad, las mismas que deberán cumplir las condiciones estipuladas en el artículo 58 de la LOPDP.

Todo cambio a las normas vinculantes debe ser comunicado a la autoridad de protección de datos personales de acuerdo a los mecanismos indicados por el responsable del tratamiento.

Para todos los casos no contemplados en la presente política o en la normativa relacionada con la protección de datos personales, se requiere la autorización de la autoridad de protección de datos personales, para realizar una transferencia internacional para lo cual se deberá garantizar documentadamente el cumplimiento de la normativa vigente.

La información de transferencias internacionales debe registrarse previamente en el A-GCI-PDP-04 Registro nacional de protección de datos personales, por parte del responsable o del encargado.

Las transferencias o comunicaciones internacionales se podrán realizar en los casos señalados en el Artículo 60 de la LOPDP, primando los casos de interés público, colaboración judicial internacional, investigación de infracciones, operaciones bancarias y bursátiles, cumplimiento de obligaciones legales o regulatorias, ejecución de contratos o medidas contractuales adoptadas por el titular, cooperación entre Estados, defensa de reclamaciones, acciones administrativas o jurisdiccionales y cuando la transferencia sea necesaria para protección de intereses vitales del titular cuando está física o jurídicamente incapacitados para dar su consentimiento.

No se podrá realizar ninguna transferencia internacional de datos personales cuando la autoridad de protección de datos personales haya emitido una resolución de no adecuación para un país u organización que no cumpla con un nivel adecuado de protección de acuerdo a lo establecido en la LOPDP.

CAPÍTULO VI: SEGURIDAD DE DATOS PERSONALES

Artículo 18.- Consideraciones Generales de la Seguridad de Datos Personales

El responsable o encargado del tratamiento de datos personales deberá encargarse de implementar la seguridad de datos personales en la institución, basados en la Ley Orgánica de Protección de Datos Personales, en esta política, en el principio de seguridad de datos personales y las “Políticas Institucionales para el sistema de gestión de seguridad de la información” (en lo que aplique para la protección de datos personales).

De manera semestral o cuando se identifique una probabilidad alta de que se materialice algún riesgo que afecte a la protección de datos personales, se debe generar el “Informe de verificación y evaluación de seguridad de datos personales”, para lo cual se deberá usar la plantilla "Informe de monitoreo y evaluación del sistema de gestión de seguridad de la información", de acuerdo al “Manual de procedimientos para verificar el cumplimiento del sistema de gestión de la seguridad de la información”, que garantice la eficiencia, eficacia y efectividad de las mismas, a todos los procesos

involucrados y componentes relacionados, que incluye aspectos técnicos, administrativos, organizativos, etc.

Así también se validará la gestión de riesgos, de acuerdo al Manual de Procedimientos para el Control y Mitigación de Riesgos de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales, utilizando como referencia el A-GCI-PDP-04 Registro nacional de protección de datos personales institucional. Los resultados deberán presentarse mediante el "Informe de verificación y evaluación de seguridad de datos personales", elaborado por el DPD y revisado por el / la Gerente de Seguridad de la Información. Este informe deberá generarse utilizando la plantilla "Informe de monitoreo y evaluación del sistema de gestión de seguridad de la información", establecida en el "Manual de procedimientos para verificar el cumplimiento del sistema de gestión de la seguridad de la información", y su aprobación será gestionada ante el "CASI" conforme a las funciones señaladas en su reglamento.

Los aspectos mínimos que debe contemplar esta revisión son:

- Medidas de anonimización, seudonomización o cifrado de datos personales: De conformidad con las "Políticas institucionales para el sistema de gestión de seguridad de la información", se debe gestionar con los propietarios de la información, los datos que se deben despersonalizar, especialmente para esos datos personales que tienen que ser consultados por otras personas en ambientes de desarrollo o pruebas, así como también los datos que requieren ser cifrados y cuya implementación depende de la Gerencia de Innovación Tecnológica, bajo la coordinación de la Gerencia de Seguridad de la Información. Los datos que deben ser anonimizados o cifrados, deben constar en el A-GCI-PDP-04 Registro nacional de protección de datos personales institucional y del A-GCI-PDP-04 Inventario de datos personales institucionales de tal manera que se gestione su implementación para lo cual, propietario de la información debe gestionarlo con las personas involucradas, entre ellas, con el personal de la Gerencia de Seguridad de la Información, Gerencia de Innovación Tecnológica, entre otras.
- Medidas para mantener la confidencialidad, integridad y disponibilidad de los datos personales: Se debe dar cumplimiento a las "Políticas institucionales para el sistema de gestión de la seguridad de la información", haciendo énfasis en el "Capítulo X: Del acuerdo de privacidad de la información y protección de datos personales", por lo que, resulta indispensable generar el A-GCI-PDP-03 De Privacidad de la Información y Protección de Datos. Se debe gestionar con los titulares de los datos, el control de accesos, la validación de la integridad de los datos y que los mismos estén disponibles cuando se lo requiera.
- Medidas dirigidas a mejorar la resiliencia técnica, física, administrativa, jurídica y a la gestión de riesgos: El "Inventario de datos personales institucionales", debe venir acompañado con una gestión adecuada de riesgos que permita evitar que se presenten, por lo que se deberá incluir el resultado del análisis de riesgos, amenazas y vulnerabilidades. Si pese a eso y aunque se han tomado acciones correctivas, los riesgos se materializan, se debe gestionar para que los datos se los restablezca lo antes posible, para lo cual se debe dar cumplimiento al "Capítulo XXIV De la gestión de incidentes de seguridad de la información", de las "Políticas institucionales para el sistema de gestión 2 y o accesos no autorizados, a más de comunicar a las personas involucradas en la protección de datos personales, se debe reflejar en el "Informe de verificación y evaluación de seguridad de datos personales", lo que permitirá plantear las acciones correctivas respectivas.
- Se debe presentar la gestión de medidas correctivas implementadas.
- En caso que se apliquen procesos automatizados, con datos personales, como por ejemplo la elaboración de perfiles crediticios para la aprobación de créditos, se debe hacer la evaluación

sistemática correspondiente, que permita comprobar la transparencia de los procesos y se garantice la protección de los datos personales.

- En el informe deben considerarse el tratamiento de datos sensibles o especiales, de tal manera que se compruebe el cumplimiento de la normativa relacionada con los datos personales.
- En el caso que la institución maneje datos públicos a gran escala, deben ser revisados para que no se de incumplimiento a la normativa y se compruebe que no se trata de datos personales confidenciales o sensibles.

Artículo 19.- Medidas de Seguridad en el Ámbito del Sector Público

Se deben considerar todas las medidas de seguridad de los datos personales, para poder enfrentar los riesgos asociados, amenazas, vulnerabilidades, accesos no autorizados, fuga o pérdida de información, alteración a la integridad de los datos, eliminación o destrucción parcial / total de los datos.

Las medidas de seguridad para la protección de los datos personales, se enmarca en garantizar la confidencialidad, integridad y disponibilidad de los datos personales y por lo tanto, se debe dar cumplimiento a las "Políticas institucionales para el sistema de gestión de seguridad de la información", que incluye los siguientes temas: Seguridad física, Seguridad de las comunicaciones y operaciones, Control de accesos, Controles por cada activo de la información con un enfoque de Gestión de riesgos de seguridad de la información, Seguridad en dispositivos de almacenamientos externos, eliminación de la información, cifrado de información, Segmentación de la red de datos, almacenamiento en la nube, intercambio de información, monitoreo de vulnerabilidades, entre otros.

Se vuelve indispensable una adecuada administración de los riesgos asociados a los datos personales, por lo que, se debe considerar esta temática para dar cumplimiento al "Capítulo XXIV: De la gestión de incidentes de seguridad de la información" de las "Políticas Institucionales para el sistema de gestión de seguridad de la información" y además del "Manual de Procedimientos para el Control y Mitigación de Riesgos de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales", que deben garantizar:

- Las particularidades del tratamiento;
- Las particularidades de las partes involucradas; y,
- Las categorías de acuerdo a la naturaleza de los datos personales y el volumen de datos personales objeto de tratamiento;
- Plazos de vigencia por categorías de los datos personales. En el análisis se debe establecer la forma de destrucción de los datos personales una vez que se cumplan los plazos.

Además, es necesario administrar una adecuada gestión de las acciones correctivas, para lo cual se debe mantener actualizado el A-GCI-PDP-02 Bitácora de acciones correctivas
En el "Informe de verificación y evaluación de seguridad de datos personales" deben constar todas las acciones realizadas para garantizar las medidas de seguridad en la protección de datos personales, de acuerdo a la normativa relacionada.

Artículo 20.- Protección de Datos Personales desde el Diseño y por Defecto
El tratamiento de los datos personales, va a ser diferente de acuerdo a su naturaleza, por lo que no será lo mismo el tratamiento que se le da a los datos personales de los clientes de crédito, que a los datos personales de los funcionarios de la institución. Esto implica que en su diseño se deben considerar todos los aspectos necesarios por tipo de datos, situación que se detalla en el capítulo III

de la presente política y el responsable o encargado del tratamiento deberá velar su cumplimiento, situación que debe reflejarse en el "Informe de verificación y evaluación de seguridad de datos personales".

Artículo 21.- Notificación de Vulneración de Seguridad

Cuando se presente una vulnerabilidad a la seguridad de los datos personales, el Gerente de Seguridad de la Información evaluará el incidente y emitirá un informe técnico correspondiente. Dicho informe será remitido al Gerente General o a su delegado formal, quien en su calidad de Responsable de Tratamiento, efectuará la notificación mediante oficio, a la Autoridad de Protección de Datos Personales y a la Agencia de Regulación y Control de las Telecomunicaciones, y a todos los involucrados en el tema, entre ellos al delegado, titular y Gerente de Seguridad de la Información.

La notificación se tiene que realizar inmediatamente o hasta el término de cinco (5) días contados desde el momento que se comprobó la vulneración de seguridad, a excepción de que sea improbable el riesgo de afectación a los derechos y libertades de las personas, en cuyo caso igual se tiene que realizar la notificación adjuntando los motivos respectivos.

Mientras que el encargado del tratamiento también realizará la notificación respectiva, de manera formal mediante memorandos / oficios, pero en un término de dos (2) días a partir de la fecha que tenga conocimiento de la afectación a la seguridad de los datos personales.

Artículo 22.- Acceso a Datos Personales para Atención a Emergencias e Incidentes Informáticos

Se puede acceder y realizar el tratamiento de datos personales, en casos de emergencias e incidentes informáticos que afecten a la vida de las personas o impacten a la continuidad del negocio de la institución, durante el tiempo necesario hasta que el riesgo de afectación a las personas o a la institución ya no sea de alto impacto. Este acceso debe ser conocido por el responsable y el encargado del tratamiento de datos personales y solo puede ser realizado por: autoridades del nivel jerárquico de la institución, Gerencia de Talento Humano, Gerencia de Innovación Tecnológica, Gerencia de Seguridad de la Información, Gerencia de Riesgos, Gerencia de Negocios Financieros y Captaciones, Gerencia de Operaciones Financieras, Gerencia de Negocios Fiduciarios y Departamento Médico; así como también instituciones externas que tengan relación con la protección de datos personales, como por ejemplo: autoridades públicas competentes, equipo de respuestas a emergencias y/o incidentes de seguridad informática, centros de operaciones de seguridad, prestadores y proveedores de seguridad de telecomunicaciones, proveedores de tecnología y de servicios de seguridad.

Artículo 23.- Garantía del Secreto de las Comunicaciones y Seguridad de Datos Personales

El proveedor de servicios de telecomunicaciones, incluyendo al proveedor externo, como a la Gerencia de Innovación Tecnológica, deben garantizar el secreto de las comunicaciones y de la seguridad de los datos personales, por lo que, no podrán realizar grabaciones o copias de la información generada en el ámbito de las telecomunicaciones, a excepción que exista una orden judicial, en cuyo caso se pueden hacer copias de los contenidos de comunicaciones específicas, de acuerdo a lo que dispongan los jueces componentes, de otro modo se aplicará las sanciones de las normativas correspondientes.

Artículo 24.- Notificación de Vulneración de Seguridad al Titular

En caso de identificar una vulnerabilidad que afecte a los derechos y libertades del titular, el Gerente de Seguridad de la Información, elaborará un informe técnico correspondiente y notificará de manera inmediata a la Gerente General o su delegado formal quien en su calidad de Responsable del Tratamiento en el término de tres (3) días a partir del momento en que se tuvo conocimiento del evento de riesgo, debe realizar la notificación correspondiente al titular, en el caso de no hacerlo se sujetará a las sanciones establecidas en la normativa respectiva (LOPDP, el reglamento asociado a la LOPDP, a la presente política).

Las notificaciones no se deben realizar en los siguientes casos:

- Siempre y cuando se compruebe que las medidas de protección aplicadas por el responsable del tratamiento de datos personales sean efectivas y por lo tanto, no afecten a las libertades y derechos del titular, situación que debe ser calificada por la autoridad de datos personales.
- Cuando se requiera un "esfuerzo desproporcionado" para tomar acciones que permitan garantizar los derechos y libertades de los titulares; sin embargo, el responsable del tratamiento de datos personales comunicará de manera pública sobre la vulneración de seguridad a los titulares.

Tanto la notificación como la aplicación de medidas "oportunas", serán consideradas como atenuantes a favor del responsable de tratamiento de datos personales.

CAPÍTULO VII: REQUERIMIENTOS DIRECTOS Y DE LA GESTIÓN DEL PROCEDIMIENTO ADMINISTRATIVO

Artículo 25.- Gestión del Procedimiento Administrativo

Requerimiento directo del titular del dato de carácter personal.-

El titular de datos personales, en cualquier momento podrá hacer solicitudes relacionadas con el tratamiento de sus datos personales (requerimientos, peticiones, quejas, reclamos, etc.), de manera formal mediante memorando u oficio o mediante el correo pdp@cfn.fin.ec, según sea el caso, las cuales estarán dirigidas al responsable de protección de datos personales, quien de manera coordinada con el encargado y el responsable gestionarán los requerimientos. Se atenderá, de forma gratuita, todas las solicitudes relacionadas con el ejercicio de sus derechos, la aplicación de principios y el cumplimiento de obligaciones por parte de todos los integrantes del tratamiento, que tengan relación con el titular. Se contará con un término de diez (10) días para contestar afirmativa o negativamente, notificar y ejecutar lo que corresponda.

Actuaciones previas.- La autoridad de protección de datos personales podrá iniciar, de oficio o a petición del titular, actuaciones previas con el fin de conocer las circunstancias del caso concreto o la conveniencia o no de iniciar el procedimiento, para lo cual se estará conforme a las disposiciones del Código Orgánico Administrativo.

Procedimiento administrativo.- Los procedimientos administrativos que viabilicen el cumplimiento de la LOPDP estarán conforme a esta ley, al procedimiento establecido en el Código Orgánico Administrativo y demás normativa emitida por la autoridad de protección de datos personales.

Artículo 26.- Medidas Correctivas, Incumplimientos e Infracciones

Es importante mencionar que el encargado (s) y/o responsable de la protección de datos personales, en caso de incumplimiento de sus funciones responderán administrativa, civil y penalmente, de conformidad con la Ley Orgánica de Protección de Datos Personales.

Medidas Correctivas:

Todas las personas involucradas en la protección de datos personales, podrán identificar vulnerabilidades e incidentes que afecten a la protección de datos personales, en cuyo caso deben ser notificados al Delegado de Protección de Datos Personales de manera oficial mediante memorando u oficios o mediante el correo pdp@cfn.fin.ec, según sea el caso, para que se proceda de acuerdo al "Capítulo XXIV: De la gestión de incidentes de seguridad de la información" de las "Políticas institucionales para el sistema de gestión de seguridad de la información".

El responsable o encargado del tratamiento de los datos personales, mantendrá el A-GCI-PDP-02 Bitácora de acciones correctivas, en la que por lo menos debe contener la siguiente información:

- Fecha de identificación de la medida correctiva;
- Detalle del riesgo, vulnerabilidad o incidente detectado;
- Detalle de los datos que fueron afectados;
- Detalle de las personas que fueron afectadas;
- Fecha de inicio de la afectación (si no se tiene certeza por lo menos se debe mencionar una fecha aproximada);
- Medio de detección;
- Nombre y rol de la persona que identificó la medida correctiva;
- Detalle del alcance de la medida correctiva (debe ser completa, clara y precisa);
- Tipo de medida correctiva (general o específica);
- Si el tipo de medida correctiva es específica, se debe identificar el titular y el proceso institucional asociado a la seguridad de los datos personales;
- Responsable de la Implementación de la medida correctiva;
- Fecha de inicio para la implementación;
- Fecha de fin de implementación:
- Fecha de comunicación de implementación a los involucrados;
- Observaciones (detallando aspectos relevantes de esta implementación y si causaron los efectos esperados).

Las medidas correctivas, pueden orientarse a corregir, revertir o eliminar conductas contrarias a una adecuada gestión de los datos personales y pueden consistir, entre otras en:

- Suspender el tratamiento de datos personales, bajo ciertas condiciones o plazos;
- Eliminar datos personales; y,
- Imponer la aplicación de medidas técnicas, jurídicas, organizativas o administrativas, que permitan el tratamiento adecuado y de acuerdo a la normativa de datos personales.

Para aplicar medidas correctivas, se deben considerar las reglas dispuestas en la Ley Orgánica de Protección de Datos Personales (artículo 66), de tal manera de definir si una infracción es leve, grave o muy grave, en cuyo caso se aplicarán las infracciones correspondientes de acuerdo a los artículos 69,70, 71 y 72.

CAPÍTULO VIII: ANEXOS

- A-GCI-PDP- 01 Política privacidad y política cookies

- A-GCI-PDP-02 Bitácora de acciones correctivas.
- A-GCI-PDP-03 De Privacidad de la Información y Protección de Datos
- A-GCI-PDP-04 Registro nacional de protección de datos personales e Inventario de datos personales institucionales.
- A-GCI-PDP-05 Bitácora de eliminación de datos personales.

CONTROL E HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO	RESPONSABLE
01		- Se incorporaron lineamientos orientados a fortalecer la claridad del documento y establecer directrices más precisas para su aplicación. -Se incorporan nuevos términos al Glosario -Se codifican anexos relacionados al documento conforme Inventario de Procesos aprobado - Se elimina la información relacionada con "Medidas Correctivas", en virtud de que estas se encuentran contempladas en la Ley Orgánica de Protección de Datos Personales y su Reglamento.	Clara Marisela Veliz Loor, Gerente de Seguridad de la Información
00	25 de mayo de 2023	Documento de referencia correspondiente a la última actualización aprobada mediante acto administrativo, establecido como versión inicial (00). A partir de esta versión se inicia el control de cambios.	

LISTADO DE RESOLUCIONES
• Regulación No. DIR-025-2023 de 25 de mayo de 2023.

CONTROL DE LA DOCUMENTACIÓN

FASE	DETALLE	FIRMA	
Elaborado por:	**Nombre:** Richard Alfonso Calderón Suárez		
	Cargo: Especialista en Gestión de Proyectos Informáticos		
	Nombre: Liz Lilibeth Pino Merchán		
	Cargo: Técnico de Administración de Recursos		
Revisado por:	**Nombre:** Clara Marisela Veliz Loor		
	Cargo: Gerente de Seguridaad de Información		
	Nombre: Christian Andrés Durán López		
	Cargo: Gerente de Normativa y Procesos		
	Nombre: Marlene Eloisa Vega Carvajal		
	Cargo: Subgerente General de Operaciones y Procesos		
		REFERENCIA	**FECHA**
Revisado por:	Pronunciamiento de la Subgerencia General Jurídica	CFN-B.P.-SGJU-2026-0136-M	26 de marzo de 2026
	Pronunciamiento de Riesgos	CFN-B.P.-GERI-2026-0143-M	26 de marzo de 2026
Aprobado por:	Directorio de la Corporación Financiera Nacional B.P.		