Cumplimiento y Ética Credicorp
**Programa Protección de Datos Personales (PDP)**
Política Corporativa de Protección de Datos Personales
Fecha de Vigencia: 07/12/2018
Fecha de Publicación: 06/12/2018

## 1. Objetivos Generales

Las empresas del Grupo Credicorp están comprometidas con la protección y privacidad de los Datos Personales de los Usuarios en cumplimiento de la Ley de Protección de Datos Personales - Ley N° 29733,su Reglamento aprobado por el Decreto Supremo N° 003-2013-JUS y sus respectivas modificatorias ("las Normas de Protección de Datos Personales"). En coherencia con ello, esta Política Corporativa tiene como objetivos:

a) Establecer los lineamientos generales para el Tratamiento y Transferencia de Datos Personales de grupos de interés tales como colaboradores, Usuarios, clientes y proveedores en todas las empresas del Grupo Credicorp.

b) Asegurar que las empresas del Grupo Credicorp cumplan las Normas de Protección de Datos Personales.

c) Hacer de conocimiento de todos los colaboradores de las empresas del Grupo Credicorp el impacto del incumplimiento de las Normas de Protección de Datos Personales.

## 2. Definiciones

a) **Activo de Información:** todo documento físico (DF), documento digital (DD) y aplicativos informáticos (APP) que tengan un valor para la empresa y/o soporten o sean parte de la actividad, proceso o giro de negocio de la organización.

a) **Aplicativo informático fuera de la custodia de la Unidad de Sistemas (APPnoIT):** todo activo de información orientado al procesamiento y administración de datos que se encuentre administrado por una Unidad, y además se encuentre alojado en la misma Unidad o en la Unidad de Sistemas. Se incluye a esta definición los archivos digitales con lógica de programación en su contenido, como, por ejemplo: macros en Excel, bases de datos en Access, flujos de trabajo en SharePoint, entre otros.

b) **Banco de Datos Personales:** conjunto organizado de Datos Personales automatizados o no, independientemente del soporte, sea este físico, magnético, digital u otros que se cree, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.

c) **Consentimiento:** autorización del Titular de los Datos Personales para que el Titular del Banco de Datos Personales realice Tratamiento y/o Transferencia de los mismos.

d) **DPDP:** Dirección de Protección de Datos Personales.

e) **Datos Personales**: aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a una persona natural, que la identifica o la hace identificable directa o indirectamente a través de medios que puedan ser razonablemente utilizados. Ej.: nombres y apellidos, DNI/RUC, pasaporte, sexo, profesión, edad, nacionalidad, fecha de nacimiento, dirección, teléfono, correo electrónico, fotografía, firma, voz, etc.

f) **Datos Sensibles:** Datos Personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, hábitos personales de la esfera más íntima,

información relativa a la salud física o mental, datos biométricos que por sí mismos pueden identificar al titular, datos referidos al origen racial y étnico, ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales, afiliación sindical, información relacionada a la salud o a la vida sexual u otras que afecten la intimidad de la persona natural.

g) **Documento digital (DD)**: todo activo de información que contenga datos en formato electrónico, y que requiere de un dispositivo informático para su acceso y consulta. Se excluye de esta definición a todo archivo digital que contenga lógica de programación en su contenido, como por ejemplo macros en Excel.

h) **Documento físico (DF):** todo activo de información que contenga datos registrados en un formato tangible tales como comprobantes de caja, documentos de control operativo, documentos activos, documentos pasivos, documentos para archivo físico, entre otros.

i) **Empresas del Grupo Credicorp:** empresas locales del Grupo Credicorp tales como el Banco de Crédito del Perú, Mibanco, Prima AFP, Pacífico Seguros, Pacífico Asiste y Credicorp Capital Perú y sus subsidiarias (Credicorp Capital SAB, Credicorp Capital SAF, Credicorp Capital Sociedad Titulizadora y Credicorp Capital Servicios Financieros).

j) **Encargado de tratamiento de Datos Personales:** Toda persona natural, jurídica de derecho privado o entidad pública que, sola o actuando conjuntamente con otra, realiza el Tratamiento de los Datos Personales por encargo del Titular del Banco de Datos Personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación. Incluye a quien realice el tratamiento sin la existencia de un banco de datos personales.

k) **Encargo de tratamiento:** Entrega por parte del titular del banco de datos personales a un encargado de tratamiento de Datos Personales en virtud de una relación jurídica que los vincula. Dicha relación jurídica delimita el ámbito de actuación del encargado de tratamiento de los Datos Personales.

l) **Flujo Transfronterizo de Datos Personales:** Transferencia internacional de Datos Personales a un destinatario situado en un país distinto al país de origen de los Datos Personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban.

m) **Titular de Datos Personales**: persona natural a quien corresponden los Datos Personales.

n) **Titular del Banco de Datos Personales**: persona natural, jurídica de derecho privado o entidad pública que determina la finalidad y contenido del Banco de Datos Personales, Tratamiento de estos y las medidas de seguridad.

o) **Transferencia:** toda transmisión, suministro o manifestación de Datos Personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del Titular de Datos Personales.

p) **Tratamiento:** cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de Datos Personales.

q) **Usuarios:** personas naturales que pueden hacer uso de ciertos servicios que ofrecen las empresas del Grupo Credicorp sin necesidad de ser clientes o tener algún contrato firmado con la empresa. Ej.: personas naturales que pagan los servicios de luz o agua en el BCP, que ingresan a oficina de venta de una empresa a pedir información sobre los productos que esta ofrece, etc.

## 3. Alcance

Las Normas de Protección de Datos Personales establecen un marco de protección para los Datos Personalesa ser contenidos y/o destinados a ser contenidos en Bancos de Datos Personales de administración pública y/o privada, cuyo tratamiento se realice por personas naturales, entidades públicas o instituciones del sector privado en el territorio nacional o en los siguientes casos:

- Se efectúe por un Encargado de Tratamiento de Datos Personales, con independencia de su ubicación, a nombre de un Titular del Banco de Datos Personalesestablecido en el territorio nacional.
- Cuando el Titular del Banco de Datos Personaleso el responsable del Tratamiento no esté establecido en territorio peruano, pero le resulte aplicable la legislación peruana por disposición contractual o del derecho internacional.
- Cuando el Titular del Banco de Datos Personales o el responsable del Tratamiento no esté establecido en territorio peruano, pero utilice medios situados en dicho territorio.

Se encuentran fuera del alcance de las Normas de Protección de Datos Personales:

- El Tratamiento realizado a información de una persona jurídica.
- Los Bancos de Datos Personalescreados por personas naturales para fines exclusivamente domésticos o relacionados con su vida privada o familiar.
- Los Bancos de datos de administración pública, cuando su tratamiento sea necesario para el cumplimiento de competencias asignadas por ley para la defensa nacional, seguridad pública y para el desarrollo de actividades en materia penal para la investigación y represión del delito.

## 4. Responsabilidades

A efectos de cumplir con las Normas de Protección de Datos Personales, los directores, las gerencias, el Oficial de Cumplimiento Normativo Credicorp los Oficiales de Seguridad de la Información, los encargados de ambos en las empresas del Grupo Credicorp, y los colaboradores en general tendrán las siguientes responsabilidades:

a) El Directorio de cada una de las empresas del Grupo Credicorp debe realizar las acciones necesarias a fin de que cada empresa adopte las medidas necesarias para asegurar el cumplimiento de lasNormas de Protección de Datos Personales y asegure el control periódico del cumplimiento de las políticas y procedimientos que implemente para tal fin.

b) Las gerencias en las empresas del Grupo Credicorp deben alinear sus procedimientos a esta Política Corporativa y adoptar las medidas necesarias para asegurar que el personal a su cargo la conozca y aplique.

c) El Oficial de Cumplimiento Normativo Credicorp y/o los encargados respectivos en las empresas del Grupo Credicorp deberán:

- Incorporar en la cultura de cumplimiento en Credicorp las obligaciones vinculadas a la protección de Datos Personales.
- Asegurar el monitoreo e investigación para el cumplimiento de esta Política Corporativa.
- Coordinar las sanciones por el incumplimiento de esta Política Corporativa.
- Asegurar el desarrollo e implementación de procedimientos que permitan asegurar el cumplimiento de las Normas de Protección de Datos Personales.
- Ser interlocutor entre la DPDP y las empresas del Grupo Credicorp.
- Gestionar la inscripción y actualización de los Bancos de Datos Personales y Flujos Transfronterizos de responsabilidad de las empresas del Grupo Credicorp ante la DPDP.
- Dar asistencia ante las inspecciones y requerimientos de la DPDP.

- Informar al Directorio sobre cualquier tema de interés relacionado al cumplimiento de esta Política Corporativa.
- En el BCP el Oficial de Cumplimiento Normativo Credicorp cumple la función de representante del Titular del Banco de Datos Personales ante la DPDP. Para el caso de las otras empresas del grupo Credicorp, será la Gerencia General quien designe al representante.

d) El Oficial de Seguridad de la Información de la matriz (BCP) o el Oficial de Seguridad de la Información en cada empresa del Grupo Credicorp, según el Gobierno de Seguridad de la Información definido en la norma 4205.010.67 Política General Corporativa de Seguridad de la Información, deberán:

a. Seguridad Informática:
- Identificarlas normas sobre la materia que hagan referencia a las Normas de Protección de Datos Personales.
- Definir las líneas base de seguridad para la infraestructura donde residen las aplicaciones.
- Definir lineamientos de seguridad para las aplicaciones que realizan Tratamiento de Datos Personales fuera de las instalaciones de cada Empresa Credicorp.
- Ejecutar capacitaciones virtuales para que los colaboradores conozcan las normas internas de seguridad técnica.
- Definir lineamientos de seguridad para el envío de Datos Personales por medios de soporte informático.
- Definir lineamientos para mantenimiento de registros de auditoría.
- Definir lineamientos para Transferencias por correo electrónico.
- Definir lineamientos para que las App No IT y Documentos Digitales cumplan con las Normas de Protección de Datos Personales.

b. Seguridad de la Información para Documentos Físicos:
- Identificarlas normas sobre la materia que se relacionen con las Normas de Protección de Datos Personales.
- Definir lineamientos de seguridad para el Tratamiento de Datos Personales en documentos físicos dentro y fuera de las instalaciones.
- Definir lineamientos de seguridad para el traslado y envío de Datos Personales por medios físicos a fin de adoptar medidas que impidan el acceso o manipulación de la información objeto del traslado.
- Definir lineamientos para que los Tratamientos de documentos físicos que contengan Datos Personales cumplan con las Normas de Protección de Datos Personales.
- Capacitar a los colaboradores sobre los controles de seguridad, definidos en las normas internas para el tratamiento de Datos Personales en documentos físicos.
- Monitorear el cumplimiento de los lineamientos de seguridad para el Tratamiento de datos personales en documentos físicos.

e) Todos los colaboradores de cada una de las empresas del Grupo Credicorp deben cumplir las Normas de Protección de Datos Personales y esta Política Corporativa, para lo cual deberán tener en cuenta las políticas que establezca la División de Cumplimiento Corporativo de cada Empresa Credicorp.

## 5. Consideraciones Generales

Al haber funciones y roles que manejan Datos Personales, las gerencias podrán disponer mayores restricciones en su unidad que las disposiciones de esta Política Corporativa, en cuyo caso prevalecerá la más exigente.

En el caso se requiera excepciones a esta política, se deberá contar con la conformidad de la Oficial de Cumplimiento Normativo Credicorp.

# 6. Lineamientos/ Políticas

## 6.1. Principios Rectores

Las empresas del Grupo Credicorp, en su calidad de Titulares de los Bancos de Datos Personales, deben cumplir con los principios rectores de la protección de datos personales, de conformidad con lo establecido en las Normas de Protección de Datos Personales y los lineamientos establecidos por la División Legal de cada una de las Empresas Credicorp y División de Cumplimiento Corporativo.

a) Principio de Legalidad

El tratamiento de los datos personales se hace conforme a lo establecido en la Ley. Se prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos.

b) Principio de Consentimiento

El Tratamiento de Datos Personales es lícito cuando el titular de los Datos Personales prestó su consentimiento libre, previo, expreso, informado e inequívoco. No se admiten fórmulas de consentimiento en las que éste no sea expresado de forma directa.

c) Principio de Finalidad

Se considera que una finalidad está determinada, cuando haya sido expresada con claridad, sin lugar a confusión y cuando de manera objetiva se especifica el objeto que tendrá el Tratamiento de los Datos Personales.

Cuando se trate de Bancos de Datos Personales que contengan datos sensibles, su creación solo puede justificarse si su finalidad además de ser legítima es concreta y acorde con las actividades o fines explícitos del Titular del Banco de Datos Personales.

Las personas que realicen el Tratamiento de algún Dato Personal, además de estar limitados por la finalidad de sus servicios, se encuentran obligados a guardar el secreto profesional.

d) Principio de Proporcionalidad

Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.

e) Principio de Calidad

Los Datos Personales contenidos en un Banco de Datos Personales, deben ajustarse con precisión a la realidad. Se presume que los datos directamente facilitados por el Titular de los mismos son exactos.

f) Principio de Seguridad

En el Tratamiento de los Datos Personales, deben adoptarse las medidas de seguridad que resulten necesarias a fin de evitar cualquier tratamiento contrario a las Normas de Protección de Datos Personales, incluyéndose en ellos a la adulteración, la pérdida, las desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio tecnológico utilizado.

g) Principio de Disposición de Recurso

Todo Titular de Datos Personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales.

h) Principio de Nivel de Protección Adecuado

Para el Flujo Transfronterizo de datos personales, se debe garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar o, por lo menos, equiparable a lo previsto por las normas de Protección de Datos Personales o por los estándares internacionales en la materia.

## 6.2. Consentimiento del Titular de Datos Personales

Las empresas del Grupo Credicorp, en su calidad de Titulares de los Bancos de Datos Personales, tienen la obligación de obtener el Consentimiento del Titular de los Datos Personales para poder realizar Tratamiento y Transferencia de sus Datos Personales, teniendo en cuenta las disposiciones de las Normas de Protección de Datos Personales y los lineamientos establecidos por la División Legal de cada una de las Empresas Credicorp y la División de Cumplimiento Corporativo. El Consentimiento debe ser:

- **Libre**: sin que medie error, mala fe, violencia o dolo que pueda afectar la manifestación de voluntad del Titular de Datos Personales, la cual debe ser voluntaria.

- **Previo**: debe ser pedido antes de la recopilación y Tratamiento de los Datos Personales.

- **Expreso e inequívoco:** debe ser manifestado en condiciones que no admitan dudas de su otorgamiento. La manifestación de voluntad del titular de datos personales puede ser verbal cuando ésta es exteriorizada oralmente de manera presencial o mediante el uso de cualquier tecnología que permita la interlocución oral; o, escrita mediante documento con firma autógrafa, huella dactilar u otro autorizado por el ordenamiento jurídico que queda o pueda ser impreso en una superficie de papel o similar (ej. “hacer clic” es una manifestación escrita válida a través de un medio digital). En el caso de los Datos Sensibles, el Consentimiento debe ser manifestado por escrito.

- **Informado**: el Titular de Datos Personalesdebe ser informado por el Titular del Banco de Datos Personalesde manera clara, expresa, sencilla y de manera previa a su recopilación sobre la finalidad para la cual sus Datos Personales serán tratados, quiénes son o pueden ser sus destinatarios, la existencia del Banco de Datos Personales en que se almacenarán, así como la identidad y domicilio del Titular del Banco de Datos Personales y, de ser el caso, del Encargado de Tratamiento de Datos Personales, el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, las consecuencias de proporcionar sus Datos Personales y de su negativa a hacerlo, el tiempo durante el cual se conserven los Datos Personales, la Transferencia de sus Datos Personales, y la posibilidad de ejercer los derechos que la Ley de Protección de Datos Personales le concede y los medios previstos para ello.

## 6.3. Excepciones al Consentimiento del Titular de Datos Personales

De acuerdo al artículo 14° de la Ley de Protección de Datos Personales, el Titular del Banco de Datos Personales o el responsable del Tratamiento no necesita obtener la autorización del Titular de los Datos Personales cuando realice Tratamiento en los siguientes supuestos:

a) Cuando los Datos Personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias.

b) Cuando sean Datos Personales contenidos o destinados a ser contenidos en fuentes accesibles al público (RENIEC, SUNAT, SBS, JNE, SUNARP, ESSALUD, Páginas Blancas, Colegios Profesionales, INFOCORP, Centrales de Riesgos, etc.)

c) Cuando sean Datos Personales sobre la solvencia patrimonial y de crédito, conforme a lo establecido en la ley.

d) Cuando medie norma para la promoción de la competencia en los mercados regulados, emitida en ejercicio de la función normativa por los organismos reguladores a que se refiere la Ley 27332 – Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicas, o la que haga sus veces, siempre que la información brindada no sea utilizada en perjuicio de la privacidad del usuario.

e) Cuando los Datos Personales sean necesarios para la preparación, celebración y ejecución de una relación contractual en la que el Titular de Datos Personales sea parte o cuando se trate de Datos Personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.

f) Cuando se realice Tratamiento de Datos Personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho Tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto profesional; o cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública, ambas razones deben ser calificadas como tales por el Ministerio de Salud; o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.

g) Cuando el Tratamiento sea efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical y se refiera a los Datos Personalesrecopilados de sus respectivos miembros, los que deben guardar relación con el propósito a que se circunscriben sus actividades, no pudiendo ser transferidos sin Consentimiento de aquellos.

h) Cuando se hubiere aplicado un procedimiento de anonimización o disociación.

i) Cuando el Tratamiento sea necesario para salvaguardar intereses legítimos del Titular de Datos Personales por parte del Titular de Datos Personales o por el Encargado de Tratamiento.

j) Cuando el Tratamiento sea para fines vinculados al sistema de prevención de lavado de activos y financiamiento del terrorismo u otros que respondan a un mandato legal.

k) Para el caso de grupos económicos conformados por empresas que son consideradas sujetos obligados a informar, conforme a las normas que regulan a la Unidad de Inteligencia Financiera, que éstas puedan compartir entre sí de sus respectivos clientes para fines de prevención de lavado de activos y financiamiento del terrorismo, así como otros de cumplimiento regulatorio, estableciendo las salvaguardas adecuadas sobre la confidencialidad y uso de la información intercambiada.

l) Cuando el Tratamiento se realiza en ejercicio constitucionalmente válido del derecho fundamental a la libertad de información.

m) Cuando el Tratamiento o la Transferencia sea en cumplimiento de una norma nacional o internacional (Ej. entrega de información a la UIF por las normas de prevención de lavado de activos y financiamiento del terrorismo, al MINTRA por las normas de seguridad y salud en el trabajo, a la SUNAT o a la IRS (EE.UU.) por las normas FATCA, etc.).

n) Otros establecidos por ley, o por el reglamento otorgado de conformidad con la Ley de Protección de Datos Personales.

## 6.4. Contratación de proveedores

Las empresas del Grupo Credicorp deben incorporar una cláusula de protección de Datos Personales en los contratos que suscriban con sus proveedores cuando éstos últimos tengan acceso a datos de Usuarios, clientes o colaboradores de la empresa, que pueden variar de acuerdo al siguiente detalle:

a) Cláusula general de proveedores.

b) Cláusula de proveedores de cobranzas.

c) Cláusula para contratos de adquisición de bases de datos.

d) Cláusula para contratos de enriquecimiento de bases de datos de la empresa Credicorp.

Cuando se trate de una alianza comercial con intercambio de Datos Personalesde Usuarios, clientes o colaboradores, la empresa del Grupo Credicorp incluirá otra modalidad de cláusula de protección de Datos Personalesen el Contrato, por la cual ambas partes se obliguen a cumplir las Normas de Protección de Datos Personales. Del mismo modo, los contratos que celebren las empresas del Grupo Credicorp entre ellas también deberán incluir una cláusula de protección de Datos Personalescuando cualquiera de ellas tenga acceso a datos de Usuarios, clientes o colaboradores de la contraparte.

## 6.5. Tratamiento de los Datos Personales de Menores de Edad

Las empresas del Grupo Credicorp solo realizarán Tratamiento de los Datos Personales de menores de edad con el previo Consentimiento de sus padres o tutores. En tal sentido, en caso los menores de edad opten por facilitar sus Datos Personales a través del sitio web, deberán solicitar el permiso correspondiente a sus padres o tutores, quienes serán considerados responsables de todos los actos realizados por los menores a su cargo.

## 6.6. Medidas de Seguridad

El Titular del Banco de Datos Personalesdebe implementar las medidas de seguridad correspondientes de acuerdo al tipo de activo de información que soporte los Datos Personales. Las empresas del grupo Credicorp deben asegurar el cumplimiento de la Política General Corporativa de Seguridad de la Información y otras políticas internas sobre el tratamiento de los Activos de Información y de los riesgos relacionados.

Dichas políticas deberán contener lineamientos para asegurar el cumplimiento de las Normas de Protección de Datos Personales, asegurando un adecuado:

a) Control de Accesos (¿quién puede acceder? ¿cuándo? ¿desde dónde? ¿qué puede hacer?)

b) Almacenamiento seguro de los Datos Personales(respaldos, áreas con acceso protegido).

c) Transferencia segura de Datos Personalesfuera de las empresas del Grupo Credicorp (medios de transporte autorizados, medidas de seguridad como cifrado para evitar accesos no autorizados, pérdida o corrupción de información durante el tránsito).

d) Traslado seguro de Datos Personalespara impedir acceso o su manipulación.

e) Tratamiento de los Datos Personales en documentos físicos (copia o reproducción de los documentos, custodia, traslado, destrucción).

## 6.7. Atención de Derechos Protegidos

Las empresas del Grupo Credicorp deben garantizar la atención de los derechos protegidos que pueda ejercer el Titular de los Datos Personales. Para ello deberán mantener disponibles canales, procedimientos e información para atender las solicitudes en los plazos establecidos por las Normas de Protección de Datos Personales.

Los derechos que puede ejercer el Titular de Datos Personalesson:

**a) Acceso/Información**

El derecho de acceso es aquel derecho a ser informado sobre cuáles son los Datos Personales incluidos en los Bancos de Datos de responsabilidad de la empresa del Grupo Credicorp, así como de las condiciones y generalidades del Tratamiento y Transferencia de los mismos.

El derecho de información es aquel derecho del Titular de Datos Personales a que se le brinde toda la información sobre la finalidad para la cual sus Datos Personales serán tratados, quiénes son o pueden ser sus destinatarios, la existencia del Banco de Datos Personales en que se almacenarán así como la identidad y domicilio del Titular del Banco de Datos Personales y, de ser el caso, del Encargado de Tratamiento de Datos Personales, de la Transferencia de sus Datos Personales, de las consecuencias de proporcionarlos y de su negativa a hacerlo, del tiempo de conservación de los mismos y de la posibilidad de ejercer los derechos que la ley le concede.

**b) Rectificación /Actualización**

Aquel derecho del Titular de Datos Personalesa actualizar, incluir o modificar sus Datos Personales. Aplica cuando los datos son parcial o totalmente inexactos, incompletos, erróneos, falsos o están desactualizados. El Titular de Datos Personales deberá especificar los datos que se desea sean rectificados, actualizados y/o incluidos, así como la corrección y/o incorporación que quiera que la empresa del Grupo Credicorp realice y deberá adjuntar los documentos de sustento necesarios para que la rectificación y/o inclusión solicitada sea procedente.

**c) Cancelación /Supresión**

Aquel derecho del Titular de Datos Personalesa solicitar la supresión o cancelación total o parcial de sus Datos Personales de un Banco de Datos Personales. Esta solicitud procede si los Datos Personales del titular hubieran dejado de ser necesarios o pertinentes para la finalidad que fueron recopilados, cuando: (i) hubiera vencido el plazo para su Tratamiento, (ii)decida revocar su Consentimiento para el Tratamiento de los mismos y (iii) en los casos en los que el Tratamiento no sea conforme a las Normas de Protección de Datos Personales.

El Titular de Datos Personalesdebe tener en cuenta que su solicitud no procederá cuando sus datos sean necesarios para ejecutar la relación contractual que mantiene con la empresa del Grupo Credicorp ni cuando deban ser conservados durante los plazos previstos en las disposiciones legales vigentes ni cuando sean conservados en virtud de razones históricas, estadísticas o científicas de acuerdo con la legislación aplicable.

**d) Oposición**

Aquel derecho del Titular de Datos Personalesa oponerse a figurar en un Banco de Datos Personales de responsabilidad de la empresa del Grupo Credicorp o al Tratamiento de su información personal cuando no hubiere prestado Consentimiento para su recopilación por haber sido tomados de fuentes de acceso al público o cuando habiendo prestado su Consentimiento, acredite la existencia de motivos fundados y legítimos relativos a una concreta situación personal que justifique el ejercicio de este derecho.

**a. Revocación**

Aquel derecho del Titular de los Datos Personales a revocar su consentimiento para el Tratamiento de sus Datos Personales en cualquier momento, sin justificación previa y siempre que dicho tratamiento se realice para finalidades adicionales a aquellas que dan lugar a su Tratamiento autorizado. En ese sentido, la solicitud de revocación no procederá si los Datos Personales son necesarios para la ejecución de la relación contractual que el Titular de los Datos Personales mantiene con la empresa del Grupo Credicorp, ni si debemos conservar los mismos por razones históricas, estadísticas o científicas de acuerdo con la legislación aplicable. Sin perjuicio del ejercicio del derecho de revocación, el Titular del Banco de Datos Personales conservará la información que corresponda por el plazo previsto en las disposiciones legales vigentes.

### 6.8. Registro de Bancos de Datos Personales y Comunicación de Flujos Transfronterizos

Las empresas del Grupo Credicorp están obligadas a inscribir en el Registro Nacional de Datos Personales, administrado por la Dirección General de Protección de Datos Personales (DPDP) del Ministerio de Justicia (MINJUS), los Bancos de Datos Personales bajo su responsabilidad, sea que se encuentren en soportes físicos (archivos, almacenes) o digitales (aplicativos, Excel, Access, etc.) y a comunicar los Flujos Transfronterizos que cada empresa del Grupo Credicorp realice.

En ese sentido, se deberá informar al Oficial de Cumplimiento Normativo Credicorp ó los encargados respectivos en las empresas del Grupo Credicorp, sobre los Bancos de Datos Personales existentes que se identifiquen y que no hayan sido registrados ante el MINJUS o que cualquier área vaya a crear a través de una iniciativa, proyecto, producto nuevo, canal nuevo, servicio nuevo, entre otros, quien analizará si ese Banco de Datos Personales es parte de algún otro banco ya registrado o si requiere registrarse como un Banco de Datos Personalesmatriz. De la misma manera, se deberá informar al Oficial de Cumplimiento Normativo Credicorp o a los encargados respectivos en las empresas del Grupo Credicorp, las transferencias internacionales de datos personales que se vayan a efectuar fin de que pueda hacerse la comunicación a la DPDP sobre los Flujos Transfronterizos de datos personales.

## 7. Presentación de reportes de potenciales violaciones a las Normas de Protección de Datos Personales y señales de alerta

El colaborador de una empresa del Grupo Credicorp deberá informar al Oficial de Cumplimiento Normativo Credicorp, los encargados respectivos en las empresas del Grupo Credicorp, a su jefe inmediato superior, o anónimamente a través del sistema Alerta GenÉtica Credicorp cualquier acto ilícito o incumplimiento de esta Política Corporativa para garantizar el cumplimiento de las Normas de Protección de Datos Personales. Las jefaturas que reciben las denuncias de sus colaboradores, deberán redirigirlas hacia la unidad de Cumplimiento de la empresa Credicorp. Cada empresa adoptará las medidas necesarias para proteger la confidencialidad de cualquier reporte, sujeto a la ley, regulaciones o procedimientos legales.

Las empresas tienen estrictamente prohibido tomar represalias contra los colaboradores que, o bien elaboran reportes de buena fe y/o participan en informar cualquier acto ilícito o incumplimiento de esta Política. Cabe precisar que cualquier colaborador que tome represalias estará sujeto a sanciones disciplinarias.

## 8. Medidas disciplinarias

Las infracciones a esta Política Corporativa o la falta de cooperación con una investigación interna podrán dar lugar a la aplicación de sanciones disciplinarias según la gravedad del caso, que pueden llegar hasta la separación del colaborador de una empresa del Grupo Credicorp de sus funciones, en concordancia con la legislación laboral; sin perjuicio de las acciones civiles y penales que pudieran corresponder.

| Documento aprobado por: | |
|---|---|
| Directorio Credicorp celebrado en sesión del 20/12/2017 | |
| Bárbara Falero | Gerencia de División Cumplimiento Corporativo |
| José Marangunich | Gerencia de Área Seguridad Corporativa |
| David Sáenz | Gerencia de División Tecnologías de Información |
| Guillermo Morales | Gerencia de División Legal y Secretaría General |
| Leandro Rocha | Gerencia de División Data & Analytics |