Cumplimiento y Ética Credicorp

Programa Protección de Datos Personales (PDP)

Política Corporativa de Protección de Datos Personales

Fecha de Vigencia: 26/05/2025

Fecha de Publicación: 22/05/2025

---

1. Objetivos Generales

Las Empresas del Grupo Credicorp están comprometidas con la protección y privacidad de los Datos Personales de los Titulares de los Datos, así como del cumplimiento de las normas de Protección de Datos Personales vigentes en cada país donde operen.

Esta Política Corporativa tiene como objetivo:

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. Marco regulatorio:

Esta política se basa en la Ley de Protección de Datos Personales N° 29733 (Ley de Datos) y su Reglamento aprobado por el Decreto Supremo N° 016-2024-JUS, vigentes en Perú, así como las demás disposiciones complementarias, sus modificatorias y aclaratorias posteriores.

Las Empresas del Grupo Credicorp que no estén domiciliadas en Perú deberán cumplir con esta Política Corporativa siempre que no contravenga con las normas vigentes en sus jurisdicciones. Toda referencia a la Ley de Datos, a “territorio nacional” o a Perú, deberá entenderse como la norma aplicable a la Empresa del Grupo Credicorp y el país en donde se encuentre domiciliada.

3. 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.
b) **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.
c) **Banco de Datos:** 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., que permita acceder sin esfuerzos desproporcionados a los Datos Personales
d) **Consentimiento:** autorización del Titular de los Datos para que el Titular del Banco de Datos realice Tratamiento y/o Transferencia de estos.
e) **DPDP:** Dirección de Protección de Datos Personales.
f) **Datos Personales:** Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados o cuando se puede verificar la identidad de la persona de manera directa o indirecta a partir de la combinación de datos. Incluye, pero no se limita a aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, de localización, identificadores en línea o de cualquier otro tipo concerniente a aspectos físicos, económicos, culturales o sociales. Ej.:

Datos elaborados por BCP para uso Interno

g) nombres y apellidos, DNI/RUC, pasaporte, sexo, profesión, edad, nacionalidad, fecha de nacimiento, dirección, teléfono, correo electrónico, fotografía, firma, voz, etc.
h) **Datos Sensibles**: Son aquellos Datos Personales relativos a: ingresos económicos, Datos Biométricos, origen racial o étnico, datos neuronales, morales o emocionales, datos relacionados a la vida afectiva o familiar, hábitos personales correspondientes a la esfera más íntima de la persona, afiliación sindical, opiniones o convicciones políticas, religiosas o filosóficas, datos relacionados con la vida sexual, salud física, mental u análogas que afecten la intimidad. Se consideran datos relacionados con la salud aquellos concernientes a la salud pasada, presente o pronosticada, ya sea física o mental. Incluye información derivada de un acto médico, grado de discapacidad e información genética.
i) **Datos Biométricos:** Datos Personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona natural que permiten o confirman la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos. Los Datos Biométricos constituyen Datos Sensibles.
j) **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.
k) **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.
l) **Elaboración de Perfiles:** forma de Tratamiento automatizado de Datos Personales que permite evaluar aspectos de una persona natural, de manera específica y continua, para analizar o predecir aspectos relativos a su rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamientos o hábitos, ubicación o movimientos.
m) **Empresas del Grupo Credicorp:** empresas peruanas y extranjeras del Grupo Credicorp, tales como el Banco de Crédito del Perú, Mibanco Perú, Prima AFP, Pacífico S.A. Entidad Prestadora de Salud y sus empresas: Clínica San Felipe S.A., Sistemas de Administración Hospitalaria S.A.C, La Esperanza del Perú S.A., Clínica Sánchez Ferrer S.A., Doctor + S.A.C., Oncocare S.A.C., Laboratorios Roe S.A., Centro Médico Odontológico Americano S.A.C., Análisis Clínicos ML S.A.C., Prosemedic S.A.C. , Pacífico Seguros, Pacífico Asiste, Grupo Crédito, Culqi, Krealo, Patronato BCP, Instituto Bicentenario, Joinnus, Yape Market S.A.C y Credicorp Capital Perú y sus subsidiarias (Credicorp Capital SAB, Credicorp Capital SAF, Credicorp Capital Sociedad Titulizadora y Credicorp Capital Servicios Financieros), Mibanco Colombia, Credicorp Colombia, Credicorp Chile, ASB Panamá, BCP Panamá, Tyba y Monokera.
n) **Encargado de Tratamiento:** Toda persona natural, jurídica de derecho privado o entidad pública que, sola o actuando juntamente con otra, realiza el Tratamiento por encargo del Titular del Banco de Datos 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.
o) **Encargo de Tratamiento:** Entrega por parte del Titular del Banco de Datos a un Encargado de Tratamiento en virtud de una relación jurídica que los vincula. Dicha relación jurídica delimita el ámbito de actuación del Encargado de Tratamiento.
p) **Fines de Tránsito:** implica que los medios no son usados para la finalidad específica de realizar el Tratamiento sino exclusivamente para hacer pasar Datos Personales de un lugar a otro.
q) **Flujo Transfronterizo:** 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.
r) **Oficial de Datos Personales:** persona designada por el Responsable de Tratamiento o Encargado de Tratamiento para la verificación, asesoramiento e implementación del cumplimiento del régimen jurídico sobre protección de Datos Personales.
s) **Portabilidad de Datos Personales o Portabilidad:** Acción a través de la cual el Titular de los Datos solicita la información que haya facilitado a un Responsable de Tratamiento, a fin de transmitirlos a otro Responsable del Tratamiento.
t) **Primer Contacto:** Contacto previo que debe realizar un Titular de un Banco de Datos con la finalidad de obtener el Consentimiento del Titular de los Datos, en caso no cuente con el

Consentimiento anteriormente, para posteriormente contactarlo para fines comerciales y publicitarios.

u) **Proveedor de Enriquecimiento de Datos:** Empresa que tiene una relación comercial con la Empresa del Grupo Credicorp, que puede pertenecer o no al grupo, y que en calidad de Titular de Banco de Datos ha obtenido el Consentimiento del Titular del Dato para transferir su información, cumpliendo siempre con la normativa de protección de Datos Personales.
v) **Responsable del Tratamiento:** Persona natural o persona jurídica de derecho privado o entidad pública que decide sobre la finalidad y medios del Tratamiento. Esta definición no se restringe al Titular del Banco de Datos, sino que incluye a cualquier persona que decida sobre el Tratamiento, aun cuando no se encuentre en un Banco de Datos.
w) **Socios Comerciales:** Empresas que tienen una relación comercial con la Empresa del Grupo Credicorp, que pueden pertenecer o no al grupo.
x) **Terceras Empresas:** Empresas a las que se puede transferir Datos Personales y cuyo listado se encuentra a disposición del Titular de los Datos. Incluye a las Empresas del Grupo Credicorp.
y) **Titular de los Datos:** Persona natural a quien corresponden los Datos Personales. Para efectos de esta política incluye a clientes, colaboradores y usuarios, siendo estos últimos aquellas personas naturales que hacen uso de los servicios que ofrecen las Empresas del Grupo Credicorp sin necesidad de ser clientes o tener algún contrato firmado con estas.
z) **Titular del Banco de Datos**: Persona natural o persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del Banco de Datos, Tratamiento de estos y las medidas de seguridad.
aa) **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 los Datos.
bb) **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.

4. Alcance

El marco de protección de los Datos Personales alcanza a aquellos a ser contenidos y/o destinados en Bancos de Datos 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, con independencia de su ubicación, a nombre de un Titular del Banco de Datos establecido en el territorio nacional o de quien sea el Responsable del Tratamiento.
- Cuando el Titular del Banco de Datos o 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 o el responsable del Tratamiento no esté establecido en territorio peruano, pero utilice medios situados en dicho territorio, salvo que tales medios se utilicen únicamente con Fines de Tránsito que no impliquen un Tratamiento. Esto comprende los siguientes supuestos:
    a. Cuando el Titular del Banco de Datos o el Responsable del Tratamiento realicen actividades relacionadas a la oferta de bienes o servicios dirigidos a los Titulares de Datos ubicados en el Perú.
    b. Cuando el Titular del Banco de Datos o el responsable del Tratamiento realicen actividades orientadas al análisis de comportamiento de los Titulares de Datos ubicados en territorio peruano, así como la Elaboración de Perfiles.

Se encuentra fuera del alcance de las normas de protección de Datos Personales el tratamiento realizado a la información de una persona jurídica.

5. 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 Tratamiento 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 las normas 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 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 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 Datos Personales del Grupo Credicorp deberá:

- Informar y asesorar al Titular del Banco de Datos o al Responsable del Tratamiento y a los empleados que se ocupen del Tratamiento respecto de las obligaciones que les incumben en virtud de las normas de protección de Datos Personales.
- Verificar e informar sobre el cumplimiento de lo dispuesto en las normas de protección de Datos Personales, así como del cumplimiento de las políticas del Titular del Banco de Datos o del Encargado de Tratamiento, incluida la asignación de responsabilidades, la sensibilización y formación del personal que participa en las operaciones de Tratamiento, y las auditorías que se realicen.
- Colaborar, en lo que resulte pertinente, con la Autoridad Nacional de Protección de Datos Personales para el cumplimiento de sus objetivos y atribuciones.
- Actuar como punto de contacto de la Autoridad Nacional de Protección de Datos Personales para cuestiones relativas al Tratamiento.
- Desempeñar sus funciones prestando la debida atención a los riesgos asociados a las operaciones de Tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines de tal Tratamiento.

e) El Oficial de Seguridad de la Información de la matriz (BCP)[1], o a quien designen sus funciones en la entidad, 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, deberá:

[1] Estas funciones son de obligatorio cumplimiento cuando la empresa cuenta con un responsable asignado.

a. Seguridad Informática:

- Identificar las 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 fuera de las instalaciones de cada Empresa del Grupo 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 AppnoIT y Documentos Digitales cumplan con las normas de protección de Datos Personales.

b. Seguridad de la Información para Documentos Físicos:

- Identificar las normas sobre la materia que se relacionen con las normas de protección de Datos Personales.
- Definir lineamientos de seguridad para el Tratamiento en DF 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 el Tratamiento 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 en documentos físicos.
- Monitorear el cumplimiento de los lineamientos de seguridad para el Tratamiento en documentos físicos.

f) Todos los colaboradores de cada una de las Empresas del Grupo Credicorp deben cumplir con:

- Hacer tratamiento adecuado de los Datos Personales a los cuales tenga acceso.
- Asegurarse de seguir con los procesos ya implementados por las áreas correspondientes.
- Utilizar los Datos Personales para la finalidad por la cual fueron recopilados y sobre la cual el Titular de los Datos nos ha dado su Consentimiento.
- Las normas y lineamientos de protección de Datos Personales.
- Esta Política Corporativa, para lo cual deberán tener en cuenta las políticas que establezca la División de Cumplimiento de cada Empresa Credicorp

g) Finalidades para la recopilación de los Datos Personales:

- Ejecución de la relación contractual (en caso de colaboradores incluye la relación laboral).
- La Empresa del Grupo Credicorp que recabó el Consentimiento podrá de manera directa o a través de sus Encargados de Tratamiento:
  - Ofrecer sus productos o servicios o de las Terceras Empresas.
  - Enviar invitaciones a sus eventos o de las Terceras Empresas.
  - Enviar información sobre los beneficios y programas de fidelización de esta o de las Terceras Empresas.
  - Realizar estudios e investigaciones de mercado, así como elaboración de perfiles.
  - Realizar el enriquecimiento de su propia Base de Datos o de las Terceras Empresas.
  - Transferir los Datos Personales a las Terceras Empresas para que estas puedan realizar las mismas finalidades descritas anteriormente.

6. Consideraciones Generales

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

En caso de que se requiera excepciones a esta Política Corporativa, se deberá contar con la conformidad del Oficial de Cumplimiento Normativo Credicorp.

7. Lineamientos/ Políticas

7.1. Principios Rectores

Las Empresas del Grupo Credicorp, en su calidad de Titulares de los Bancos de Datos, deben cumplir con los principios rectores de 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 continuación, enumeramos dichos principios:

a) Principio de Legalidad

El Tratamiento 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 es lícito cuando el Titular de los Datos 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

Los Datos Personales deben ser recopilados para una finalidad determinada. 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.

Cuando se trate de Bancos de Datos 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.

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 debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.

e) Principio de Calidad

Los Datos Personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopilados. Se presume que los datos directamente facilitados por el Titular de los Datos son exactos.

f) Principio de Seguridad

En el Tratamiento, deben adoptarse las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los Datos Personales. Las medidas de seguridad deben ser apropiadas para el tratamiento que se vaya a efectuar y con la categoría de Datos Personales que se trate.

g) Principio de Disposición de Recurso

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

h) Principio de Nivel de Protección Adecuado

Para el Flujo Transfronterizo, 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.

i) Principio de Transparencia

El Tratamiento debe ser informado de manera clara, accesible y comprensible para el Titular de los Datos. Este principio garantiza que el titular sea plenamente consciente de las condiciones del Tratamiento, de los derechos que puede ejercer y de las disposiciones establecidas en el artículo 18 de la Ley de Datos.

j) Principio de Responsabilidad Proactiva

En el Tratamiento, deben implementarse medidas legales, técnicas y organizativas que aseguren el cumplimiento efectivo de la normativa aplicable. Además, el titular del Banco de Datos o el Responsable del Tratamiento debe estar en capacidad de demostrar dicho cumplimiento.

7.2. Consentimiento del Titular de Datos Personales

Las Empresas del Grupo Credicorp, en su calidad de Titulares de los Bancos de Datos, tienen la obligación de obtener el Consentimiento del Titular de los Datos para poder realizar el Tratamiento y la Transferencia, 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 del Grupo 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 los Datos, la cual debe ser voluntaria. No se puede condicionar la prestación de un producto o servicio al otorgamiento del Consentimiento.
- **Previo**: debe ser pedido antes de la recopilación y Tratamiento.
- **Expreso e inequívoco:** debe ser manifestado en condiciones que no admitan dudas de su otorgamiento. La manifestación de voluntad del Titular de los Datos 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 necesariamente manifestado por escrito.
- **Informado**: el Titular de los Datos debe ser informado por el Titular del Banco de Datos de 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 en que se almacenarán, así como la identidad y domicilio del Titular del Banco de Datos y, de ser el caso, del Encargado de Tratamiento, 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, la existencia de decisiones automatizadas, incluida la Elaboración de Perfiles, y se transmita información relativa a las consecuencias para el titular del dato personal, y la posibilidad de ejercer los derechos que la Ley de Protección de Datos Personales le concede y los medios previstos para ello.

  Adicionalmente, se podrá recabar el Consentimiento de los Titulares de los Datos a través del Primer Contacto. Una vez que se obtengan los Datos Personales de un Titular de los Datos de forma lícita, estos pueden ser utilizados una sola vez para solicitar su Consentimiento para el Tratamiento de sus Datos Personales con fines de publicidad y/o prospección comercial. El Consentimiento recabado a través del Primer Contacto también debe ser libre, previo, expreso, inequívoco e informado.

En el supuesto en que los Datos Personales utilizados para efectuar esta figura no hayan sido recopilados de forma directa del Titular de los Datos, se deberá de estar en condiciones de informar en el Primer Contacto y a requerimiento del titular de los Datos la fuente de recopilación de estos.

Si el Titular de los Datos otorga su Consentimiento para usos adicionales durante el Primer Contacto, se podrá ofrecer publicidad durante la segunda parte de la llamada. En caso el Titular de los Datos no otorgue su Consentimiento para fines comerciales, no podrá a ser contactado nuevamente bajo la misma figura con el objetivo de recabar su Consentimiento.

Las Empresa del Grupo Credicorp son responsables por el Tratamiento en el proceso de prospección de sus productos y/o servicios, sea cual fuere el medio utilizado. Las empresas que sean contratadas para contactar al Titular de los Datos cumplen el rol de Encargados de Tratamiento.

7.3. Revocación del Consentimiento

El Titular de los Datos tiene derecho a revocar su Consentimiento para el Tratamiento 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. La solicitud de revocación debe poder llevarse a cabo a través de mecanismos fácilmente accesibles e incondicionales, sencillos, rápidos y gratuitos y debe atenderse en un plazo máximo de 10 días hábiles, durante dicho plazo es necesario que se adecuen los nuevos tratamientos y aquellos que estuvieran en proceso de efectuarse. Sin embargo, dicha solicitud de revocación no procederá si los Datos Personales son necesarios para la ejecución de la relación contractual que el Titular de los Datos mantiene con la Empresa del Grupo Credicorp, ni si se deben 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 conservará la información que corresponda por el plazo previsto en las disposiciones legales vigentes.

7.4. Excepciones al Consentimiento del Titular de Datos Personales

El Titular del Banco de Datos o el responsable del Tratamiento no necesita obtener la autorización del Titular de los Datos cuando realice Tratamiento en los siguientes supuestos:

a) 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.)

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

c) 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.

d) Cuando los Datos Personales sean necesarios para la preparación, celebración y ejecución de una relación contractual en la que el Titular de los Datos sea parte (incluye procedimientos de cobranza de los productos o servicios contratados) 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.

e) Cuando se realice Tratamiento 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.

f) Cuando el Tratamiento sea efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical y se refiera a los Datos Personales recopilados 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.

g) Cuando se hubiere aplicado un procedimiento de anonimizar o disociación.

h) Cuando el Tratamiento sea necesario para salvaguardar intereses legítimos del Titular de los Datos por parte del Titular del Banco de Datos o por el Encargado de Tratamiento.

i) 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.

j) 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.

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

l) 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.).

m) Otros establecidos por ley, o por el reglamento otorgado de conformidad con las normas de Protección de Datos Personales.

7.5. Contratación de proveedores y Socios Comerciales

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 Personales de usuarios, clientes o colaboradores de la empresa. Dichos proveedores podrán brindar servicios específicos a nombre y por encargo de la Empresa (Encargado del Tratamiento) o servicios de venta de información (Proveedor de Enriquecimiento de Datos).
Asimismo, frente a cualquier subcontratación que los proveedores -como Encargados de Tratamiento- realicen, las Empresas del Grupo Credicorp mantendrán la responsabilidad del Tratamiento.
En ese sentido, las cláusulas de protección de Datos Personales, según el tipo de contratación deberán contener:

a) Para el caso de una relación de una Empresa del Grupo Credicorp con un **Encargado de Tratamiento**:

- Compromiso de observancia de las normas en materia de Datos Personales por parte del proveedor.
- Posibilidad de efectuar auditorías al proveedor a fin de verificar el cumplimiento de las obligaciones asumidas en materia de protección y Tratamiento.
- Compromiso de mantener la confidencialidad de la información remitida.
- Compromiso de eliminar la información transferida una vez culminada la relación contractual.
- Indicación de trasladar toda solicitud de derechos ARCO que sea presentada ante el encargado a la Empresa del Grupo Credicorp con quien celebró el contrato de manera inmediata y en un plazo no mayor a 3 días hábiles.

- Prohibición de subcontratar a otra empresa sin autorización expresa y por escrita de la Empresa del Grupo Credicorp.
- Indicación de informar de manera inmediata cualquier incidente de seguridad relacionado con los Datos Personales que le fueron compartidos

b) Para el caso de una relación de una Empresa del Grupo Credicorp con un **Proveedor de Enriquecimiento de Datos**:

- Reconocimiento de que es el proveedor quien obtiene los Datos Personales que entrega a la empresa, siendo único responsable por su licitud.
- Indicación de que el proveedor cuenta con los Consentimientos, autorizaciones y permisos requeridos por las normas en materia de Datos Personales de manera previa a la Transferencia o, en su defecto, se encontrará en alguno de los supuestos de excepción contemplados en Ley de Datos.
- Compromiso de que el proveedor realizará todos los esfuerzos necesarios para asegurar que la información que transferirá corresponde al Titular de los Datos del cual se ha solicitado el enriquecimiento de su información.
- Facultad para verificar si los proveedores cuentan con el Consentimiento del Titular de los Datos para compartir la información (pe., a través de muestreos)
- Facultad de solicitar evidencia documentaria sobre la procedencia de la información adquirida (comprobación de fuentes lícitas)

c) Para el caso de **convenios de alianzas comerciales, en donde los Socios Comerciales se transfieran Datos Personales entre sí**:

- Compromiso de observancia de las normas en materia de Datos Personales por parte de los Socios Comerciales.
- Compromiso de eliminar la información transferida una vez culminada la relación contractual.
- Prohibición de subcontratar a otra empresa sin autorización expresa y por escrita del socio comercial.
- Declaración de que los Datos Personales o información que utilicen a efectos de ejecutar la alianza comercial han sido adquiridos válidamente de conformidad con las normas de protección de Datos Personales.
- Indicación de que las partes se encuentran autorizadas para utilizar y tratar los Datos Personales con la finalidad de ejecutar la alianza comercial, así como para transferirlos al Socio Comercial.

Cuando se trate de una alianza comercial con intercambio de Datos Personales de Usuarios, clientes o colaboradores, la Empresa del Grupo Credicorp incluirá otra modalidad de cláusula de protección de Datos Personales en 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 Personales cuando cualquiera de ellas tenga acceso a datos de Usuarios, clientes o colaboradores de la contraparte.

Asimismo, cuando se acuerde entre **Socios Comerciales** el intercambio de Datos Personales se deberá verificar previamente que se cuenta con el Consentimiento del Titular de los Datos para efectuar dicha Transferencia, salvo que dicho intercambio sea necesario para ejecutar una relación contractual celebrada con el Titular de los Datos.

Del mismo modo, se deberá pactar con los Socios Comerciales canales y mecanismos seguros de transferencia de información a fin de garantizar la seguridad, integridad y confidencialidad de los Datos Personales transferidos.

7.6. Tratamiento de los Datos Personales de Menores de Edad

Las Empresas del Grupo Credicorp solo podrán realizar Tratamiento de los Datos Personales de menores de catorce años 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.

En el caso de los mayores de catorce y menores de dieciocho años, de acuerdo con su capacidad, pueden otorgar el Consentimiento para el tratamiento de sus Datos Personales siempre que la información proporcionada haya sido expresada en un lenguaje comprensible para ellos, conforme a la normativa de la materia.

Las Empresas del Grupo Credicorp que realicen Tratamiento de información en plataformas o servicios en el entorno digital deben realizar esfuerzos razonables para verificar la identidad de quienes otorgan el Consentimiento y la edad de estos teniendo en cuenta la tecnología disponible.

7.7. Tratamiento de Datos Personales mediante sistemas de videovigilancia

Las Empresas del Grupo Credicorp realizarán Tratamiento captados mediante sistemas de videovigilancia únicamente para finalidades relacionadas a seguridad y/o control laboral, de acuerdo con las normas aplicables.

A efectos de cumplir con el principio de proporcionalidad, el Tratamiento debe ser adecuado, pertinente y no excesivo con relación a las finalidades que justificaron su recopilación. En ninguna circunstancia se colocarán sistemas de grabación o captación de sonido en los lugares destinados al descanso o esparcimiento de los colaboradores, como vestuarios, servicios higiénicos o análogos.

En todos los casos, se deberá informar a los Titulares de los Datos sobre la captación y/o grabación de las imágenes y/o sonidos. Dicha medida se cumple con el despliegue de carteles informativos en todas las zonas videovigiladas, así como también poniendo a disposición de los Titulares de los Datos Personales un informativo adicional con la información requerida por el artículo 18 de la LPDP.

El alcance de la ubicación y contenidos de los carteles informativos deberá considerar las pautas establecidas en la Directiva No. 01-2020-JUS/DGTAIPD, Directiva para el Tratamiento mediante sistemas de videovigilancia.

El Titular del Banco de Datos deberá registrar el banco de datos de videovigilancia ante la Autoridad Nacional de Protección de Datos Personales y deberá almacenar los Datos Personales por un plazo de treinta (30) días y hasta un plazo máximo de sesenta (60), salvo disposición distinta en normas sectoriales.

Las Empresas del Grupo Credicorp podrán emplear Encargados de Tratamiento quienes realizarán Tratamiento por cuenta de ellas, en cuyo caso se formalizará un contrato/ convenio/ documento de acuerdo con lo establecido en esta Política. Los Datos Personales que captemos mediante sistemas de videovigilancia no serán transferidos a terceros, salvo se cuente con el Consentimiento de los Titulares de los Datos, sea requerido por una autoridad competente y/o exista una obligación legal que lo autorice.

Las Empresas del Grupo Credicorp deben asegurar la confidencialidad de los Datos Personales captados mediante sistemas de videovigilancia para lo cual deben prohibir el acceso al personal no autorizado y establecer acuerdos de confidencialidad con el personal que controla o tendrá acceso a los sistemas de videovigilancia.

En cumplimiento del principio de seguridad, el Titular del Banco de Datos debe adoptar las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos y evitar su alteración, pérdida, Tratamiento o acceso no autorizado.

7.8. Medidas de Seguridad

El Titular del Banco de Datos debe implementar las medidas de seguridad correspondientes de acuerdo con el 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 Personales fuera 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 Personales para impedir acceso o su manipulación.

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

Además, el Titular del Banco de Datos debe contar con un documento de seguridad el cual debe ser aprobado formalmente y contar con fecha cierta y debe contener como mínimo los procedimientos de gestión de accesos, la gestión de privilegios y la verificación periódica de los privilegios asignados referentes a los sistemas de información, incluyendo, plataformas tecnológicas, aplicaciones móviles, motores de bases de datos, entre otros, empleados para realizar el Tratamiento. El documento de seguridad es de obligatorio cumplimiento para todos los colaboradores que tengan acceso a los sistemas de información. Del mismo modo, el Titular del Banco de Datos debe implementar medidas técnicas destinadas a aplicar procesos tecnológicos que restrinjan el acceso de los Datos Personales únicamente a colaboradores y Encargados de Tratamiento cuando su Tratamiento sea necesario y garantice la integridad y seguridad de estos.

En caso se produzca un incidente de seguridad de Datos Personales que (i) genere exposición de grandes volúmenes de estos, (ii) que pueda afectar a un gran número de personas, (iii) cuando se trate de datos sensibles o (iv) cuando se produzca un perjuicio evidente a otros derechos o libertades, se deberá notificar ello a la Autoridad de Datos como máximo dentro de las 48 horas posteriores a haber tomado conocimiento.

Si la notificación se realiza después de las 48 horas, esta debe incluir una justificación detallada y/o el sustento probatorio que explique la demora, incluso si el incidente ha sido subsanado o resuelto internamente.

La notificación del incidente de seguridad debe señalar y describir como mínimo (i) la naturaleza del incidente de seguridad, (ii) el nombre y los datos de contacto del Oficial de Datos Personales o de otro punto de contacto, (iii) las posibles consecuencias del incidente, y (iv) las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad.

Además, si se advierte un incidente de seguridad de Datos Personales que afecte al titular de estos en otros de sus derechos, debe comunicárselo dentro de las 48 horas en un lenguaje sencillo y claro, así como de las medidas adoptadas para mitigar sus efectos. Si la comunicación se efectúa luego de las 48 horas, debe justificarse la dilación.

En caso de que el incidente de seguridad se desarrolle en el entorno digital, la notificación también se debe realizar al Centro Nacional de Seguridad Digital conforme a lo establecido en el Decreto de Urgencia 7-2020.

7.9. 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. 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
En el supuesto en el cual la solicitud de ejercicio de derechos protegidos sea presentada ante el Encargado del Tratamiento, este cuenta con la obligación de remitir de manera inmediata o en un máximo de tres (3) días dicha solicitud a la Empresa del Grupo Credicorp con la que contrató.

Los derechos que puede ejercer el Titular de los Datos dependerán la regulación vigente de cada país donde realicemos el tratamiento. A continuación, definimos los principales derechos:

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 estos.
El derecho de información es aquel derecho del Titular de los Datos 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 en que se almacenarán así como la identidad y domicilio del Titular del Banco de Datos y, de ser el caso, del Encargado de Tratamiento, 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 los Datos a actualizar, incluir o modificar sus Datos Personales. Aplica cuando los datos sean parcial o totalmente inexactos, incompletos, erróneos, falsos o estén desactualizados. El Titular de los Datos 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 atendida.

c) **Cancelación /Supresión**
Aquel derecho del Titular de los Datos a solicitar la supresión o cancelación total o parcial de sus Datos Personales de un Banco de Datos. 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 estos y (iii) en los casos en los que el Tratamiento no sea conforme a las Normas de Protección de Datos Personales.
El Titular de los Datos debe 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 Personales a oponerse a figurar en un Banco de Datos 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.

e) **Portabilidad de Datos Personales**
En el caso que la regulación local de la entidad aplique el derecho de Portabilidad. El Titular de Datos Personales puede solicitar recibir los datos sobre sí mismo que haya facilitado a un

responsable de Banco de Datos, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable o Titular de Banco de Datos cuando: (i) el tratamiento esté basado en el Consentimiento o en una relación contractual en la que el titular del dato es parte; o, (ii) el tratamiento se ejerza mediante medios automatizados.

Los datos derivados, inferidos o construidos -es decir, aquellos datos que han sido sometidos a por lo menos un proceso de personalización, categorización o Elaboración de Perfiles- pueden ser objeto de Portabilidad siempre que la Empresa del Grupo Credicorp así lo determine.

Al ejercer la Portabilidad, el Titular de los Datos tiene derecho a que sus datos se transmitan directamente de un responsable o Titular de Banco de Datos a otro cuando ello sea técnicamente posible. Esto no implica que se imponga una carga financiera o técnica excesiva o irrazonable a las Empresa del Grupo Credicorp.

La transferencia de esta información debe realizarse a través de un medio automatizado que garantice la seguridad e integridad de la información.

f) **Tratamiento objetivo de Datos Personales**

El Titular de los Datos tiene derecho a no ser objeto de decisiones, automatizadas o no, que le produzcan efectos jurídicos, discriminación o le afecten de manera significativa, incluyendo aquellas que se basen únicamente en tratamientos automatizados destinados a evaluar, analizar o predecir, sin intervención humana, determinados aspectos personales del mismo. Por ejemplo, su rendimiento profesional, situación económica, estado de salud, orientación o identidad sexual, entre otros. Se exceptúan los casos en lo que ello ocurra en el marco de la negociación, celebración o ejecución de un contrato.

Cuando se traten Datos Personales como parte de un proceso de toma de decisiones sin participación del Titular de los Datos, la Empresa del Grupo Credicorp informará este tratamiento mediante su política de privacidad. El Titular de los Datos debe encontrarse en todos los casos en la posibilidad de defender su punto de vista sobre las decisiones tomadas sobre la base de sus Datos Personales a fin de salvaguardar su legítimo interés, sin perjuicio de ejercer los demás derechos establecidos en la presente sección.

7.10. Registro de Bancos de Datos y Comunicación de Flujos Transfronterizos

Las Empresas del Grupo Credicorp están obligadas a inscribir en el Registro Nacional de Datos Personales, administrado por la DPDP, los Bancos de Datos 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 Datos Personales del Grupo Credicorp o los encargados respectivos en las Empresas del Grupo Credicorp, sobre los Bancos de Datos 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 es parte de algún otro banco ya registrado o si requiere registrarse como un Banco de Datos matriz. De la misma manera, se deberá informar al Oficial de Datos Personales del Grupo Credicorp o a los encargados respectivos en las Empresas del Grupo Credicorp, las Transferencias internacionales de Datos Personales que se vayan a efectuar a fin de que pueda hacerse la evaluación del país hacia donde se transferirán los Datos Personales (observando lo previsto en las normas de protección de Datos Personales) y la comunicación a la DPDP sobre los Flujos Transfronterizos de Datos Personales.

En el caso de que el país no cuente con un nivel adecuado de protección de Datos Personales de acuerdo con las normas de protección de Datos Personales, las empresas de Grupo Credicorp deberán otorgar garantías para el Tratamiento adecuado de estos. Por ejemplo: cláusulas contractuales modelos u otros instrumentos jurídicos donde se establezcan por lo

menos las mismas obligaciones a las que se encuentra sujeto en el Perú, así como las condiciones en las que el Titular de los Datos consintió el Tratamiento de sus Datos Personales.

7.11. Tratamiento de Datos Biométricos

El Titular del Banco de Datos debe únicamente tratar Datos Biométricos cuando este resulte proporcional, estrictamente necesario y no excesivo con la finalidad del tratamiento.
El tratamiento de Datos Biométricos se ciñe a las reglas de Consentimiento y las excepciones establecidas en las normas de protección de Datos Personales (acápites 7.2, 7.3 y 7.4 del presente documento). Sin embargo, al tratarse de un Dato Sensible, si el tratamiento amerita el Consentimiento del Titular de los Datos Biométricos, este Consentimiento debe ser recabado por la Empresa del Grupo Credicorp mediante un medio escrito como, por ejemplo, un click de aceptación en un sitio web o una firma electrónica.
Este tratamiento amerita, por su sensibilidad, un nivel mayor de protección. Por ello, es obligación de las Empresas del Grupo Credicorp establecer, implementar y mantener medidas técnicas, organizativas y legales necesarias y suficientes para garantizar la seguridad de los Datos Biométricos en su máxima expresión, evitando su alteración, pérdida, tratamiento o acceso no autorizado.
En ese sentido, de acuerdo con el tratamiento de Datos Biométricos a realizar, las Empresas del Grupo Credicorp deberán definir las medidas de seguridad dirigidas a garantizar, durante todo el ciclo del tratamiento de Datos Biométricos, la disponibilidad, integridad y confidencialidad de los Datos Personales que administran, a fin de evitar su adulteración, pérdidas o tratamiento no autorizado.

7.12. Evaluación de impacto relativo a la protección de Datos Personales

La Evaluación de Impacto relativa a la protección de Datos Personales es un mecanismo de responsabilidad proactiva que permite al Titular del Banco de Datos o al responsable del tratamiento analizar previamente los riesgos asociados al manejo de dicha información. Este análisis, que es facultativo, tiene como objetivo mitigar posibles impactos negativos y puede funcionar como un atenuante de responsabilidad administrativa.

Esta evaluación se realiza de manera previa al Tratamiento, especialmente en casos de información sensible, tratamiento con fines de perfilado, datos de personas en situación de vulnerabilidad (como menores de edad, integrantes de pueblos indígenas en aislamiento o contacto inicial, o personas con discapacidad), tratamiento de grandes volúmenes de datos, o cualquier otro supuesto indicado por la Autoridad Nacional de Protección de Datos Personales.

7.13. Consideraciones adicionales sobre Inteligencia Artificial Cognitiva y Generativa

Para el caso de propuestas que se impulsen dentro de las Empresas del Grupo Credicorp con el objetivo de implementar una acción específica como modificar un proceso, iniciar un proyecto, cambiar un producto lanzar un nuevo producto, entre otros, utilizando componentes de Inteligencia Artificial se debe tener en cuenta de manera complementaria los principios y lineamientos de privacidad y de seguridad establecidos en la Política Corporativa de Inteligencia Artificial responsable. Los cuales asegurarán la privacidad, proporcionalidad y el tratamiento objetivo de los Datos Personales.

Los términos que se encuentren en mayúsculas y que no estén definidos en esta política, se encuentran definidos en la Política Corporativa de Inteligencia Artificial Responsable (indicar número de política).

8. 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 y Oficial de Datos Personales del Grupo Credicorp, a 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 del Grupo 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 Corporativa. Cabe precisar que cualquier colaborador que tome represalias estará sujeto a sanciones disciplinarias.

9. 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 sus funciones de una Empresa del Grupo Credicorp, en concordancia con la legislación laboral; sin perjuicio de las acciones civiles y penales que pudieran corresponder.

Documento aprobado por:
Directorio celebrado en la sesión del 29/09/2021 y 16/04/2025
Gerencia de Área Seguridad Corporativa, Inteligencia & Crimen Cibernético
Gerencia de División Legal y Secretaría General
Gerencia de División Data & Analytics
Chief Data Officer Credicorp
Gerencia de División de Riesgos No Financieros
Gerencia de Cumplimiento Normativo