



**INTERCORP**

**POLÍTICA CORPORATIVA DE PROTECCIÓN DE DATOS PERSONALES**

## Política Corporativa de Protección de Datos Personales

### 1. Objetivo y alcance

La presente Política Corporativa de Protección de Datos Personales (en adelante, la “Política”) tiene como objetivo establecer los lineamientos generales y específicos para contribuir a la correcta gestión, procesamiento y confidencialidad de la información de los accionistas, directores, colaboradores, proveedores de servicios, clientes y socios de negocio relacionados con Intercorp y las empresas del Grupo Intercorp (en adelante, la(s) Empresa(s)).

El presente documento es aplicable a todos los bancos o bases de datos personales o información destinada a estar contenida en bancos o bases de datos de las Empresas, así como al tratamiento de dichos bancos o bases de datos por parte de Intercorp o por parte de terceros que traten datos personales en su carácter de encargados. Estas disposiciones también serán aplicables a datos personales que no se encuentren contenidos en bancos de datos personales.

Todos los colaboradores de las Empresas, así como todos los terceros con quienes se vinculen en el ejercicio regular de su negocio y tengan acceso o realicen tratamiento de datos personales se encuentran sujetos al cumplimiento de la Política.

Las Empresas garantizan el derecho fundamental a la protección de datos personales y promueven el cumplimiento de lo establecido en la Ley No. 29733 – Ley de Protección de Datos Personales, el Reglamento establecido mediante Decreto Supremo No. 016-2024-JUS y Directiva de Seguridad de la Información, aprobada por la Resolución Directoral No. 019-2013 y sus modificatorias. Los lineamientos establecidos en esta Política siguen los principios rectores establecidos en el marco legal peruano.

La presente Política es de cumplimiento obligatorio para todos los directores, colaboradores, proveedores de servicios, así como para cualquier socio de negocio, independientemente de su posición, ubicación geográfica o el nivel de responsabilidad que tengan.

### 2. Compromisos

Las Empresas se encuentran comprometidas a cumplir con la legislación vigente en Perú en materia de protección de datos personales, la cual obliga a Intercorp a cumplir determinadas exigencias, fundamentalmente referidas a:

- La recopilación y el tratamiento de datos personales.
- La calidad y la seguridad de la información.
- Los derechos de las personas con respecto a los datos personales sobre sí mismos.

En este contexto, se encuentran comprometidas con la protección, el manejo y el tratamiento adecuado de los datos personales a los que tienen acceso en la operación regular de sus negocios, ya sean datos de trabajadores, clientes,

proveedores de servicios, terceros, usuarios de sitios web, de aplicaciones móviles, de teléfono, de redes sociales y/o cualquier otro canal de contacto y/o contratación dispuestos por las Empresas, entre otros.

La presente Política de protección de datos personales recoge las prácticas desarrolladas por las Empresas para la recolección, almacenamiento y tratamiento de datos personales a fin de asegurar el respeto por los derechos de sus titulares, así como el cumplimiento del marco normativo vigente.

La Política podrá ser complementada con especificaciones contenidas en reglamentos corporativos o directrices adicionales que desarrollen lo establecido en el presente documento siempre que se encuentren alineadas con sus principios rectores.

### 3. Definiciones

<b>Datos Personales</b>	Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.
<b>Tratamiento de datos personales</b>	Es cualquier operación o conjunto de operaciones, automatizados o no, que se realicen sobre los datos personales o conjuntos de datos personales. Los tratamientos pueden ser, sin limitarse a éstos, los siguientes: cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, acceso, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, selección, grabación, confrontación, disociación, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación, uso o interconexión de los datos personales.
<b>Titular de datos personales</b>	Persona natural a quien corresponden los datos personales.
<b>Titular del banco de datos o responsable de tratamiento</b>	Persona natural, persona jurídica de derecho privado o entidad pública que decide sobre la finalidad y medios del tratamiento de datos personales, aun cuando dicha información no se encuentre en un banco de datos personales organizado.
<b>Encargado del tratamiento</b>	Persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por cuenta o encargo del titular del banco de datos personales o el responsable de tratamiento.

<b>Datos Sensibles</b>	<p>Datos personales constituidos por los 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; e información relacionada a la salud o a la vida sexual.</p> <p>Asimismo, aquella información relativa a datos genéticos de la persona natural, datos neuronales, datos morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la afiliación sindical, salud física o mental u otras análogas que afecten su intimidad.</p>
<b>Banco de Datos</b>	<p>Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea físico, magnético, digital óptico u otros que se creen, cualquiera que fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.</p>
<b>Oficial de Datos Personales</b>	<p>Es la persona designada por el responsable de tratamiento o encargado del tratamiento de datos personales para la verificación, asesoramiento e implementación del cumplimiento del régimen jurídico sobre protección de datos personales.</p> <p>Debe reunir las cualidades y cumplir las obligaciones señaladas en el artículo 39 y siguientes del Decreto Supremo No. 016-2024-JUS.</p>
<b>Derechos ARCO</b>	<p>Son los derechos que tiene el titular de datos personales frente al titular del Banco de Datos o al encargado del tratamiento de sus datos. Los Derechos ARCO (Derechos de Acceso (incluyendo portabilidad), Rectificación, Cancelación y Oposición) son personalísimos y gratuitos.</p>
<b>Empresas o Grupo</b>	<p>Son todas las empresas que integran el grupo Intercorp, y aquellas sobre las cuales, sin integrar el grupo, Intercorp tiene injerencia en su administración, independientemente de su lugar de constitución.</p>
<b>Transferencia de datos personales</b>	<p>Es la comunicación de datos personales dentro o fuera del territorio nacional realizada a persona distinta al titular de los datos personales.</p>

<b>Incidente de seguridad de datos personales:</b>	Toda vulneración de la seguridad que ocasione la destrucción, pérdida, alteración ilícita de los datos personales o la comunicación o exposición no autorizada a dichos datos
----------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

La presente política adopta las definiciones establecidas en la Política Corporativa Marco de Integridad y Cumplimiento que le fueran aplicables.

#### **4. Oficial de Datos Personales**

El dato de contacto del Oficial de Datos Personales de Intercorp será publicado una vez que el mismo sea debidamente designado<sup>1</sup>.

#### **5. Confidencialidad**

Los datos personales a los que los colaboradores de las Empresas y/o terceros tengan acceso tienen carácter confidencial y no podrán ser divulgados, comunicados ni compartidos con terceros sin contar con el consentimiento previo del titular del referido dato, salvo cuando sean necesarios para llevar a cabo alguna de las etapas de una relación comercial y/o alguna de las excepciones admitidas por la legislación.

Todas las personas que intervengan en el tratamiento de los datos personales estarán obligadas a guardar el secreto profesional y a mantener la confidencialidad respecto de los mismos. Dicha obligación se mantendrá aún después de finalizada la relación que une a esas personas con Intercorp.

#### **6. Bancos de Datos Personales**

Las Empresas se comprometen, conforme a las disposiciones legales aplicables en Perú, a inscribir los bancos de datos personales de los cuales son responsables o titulares en el registro estatal pertinente.

#### **7. Derechos de los Titulares de datos personales**

Las Empresas contarán con un procedimiento sencillo y gratuito de atención de los derechos de los titulares de los datos personales contemplados en la legislación, entre ellos el derecho de acceso (incluyendo portabilidad), rectificación, cancelación y oposición, los cuales podrán ser ejercidos en cualquier momento.

Por lo tanto, las Empresas realizarán las acciones necesarias para informar al titular de los datos personales sobre los derechos conferidos por la legislación, atendiendo de manera oportuna y dentro de los plazos todas las solicitudes y requerimientos relacionados con dichos derechos.

---

<sup>1</sup> La designación del Oficial de Datos Personales recién será exigible a partir del 30.11.2025.

La eliminación de los datos personales no procederá cuando exista una obligación legal de conservación de los datos personales en la legislación vigente.

Los titulares de los derechos podrán iniciar sus solicitudes por medio de una comunicación a la siguiente dirección de correo electrónico: [datos@colectivo23.com](mailto:datos@colectivo23.com)

Las Empresas llevarán un registro de las solicitudes de ejercicio de derechos planteadas por cada titular de datos personales.

El ejercicio de derechos de los titulares de los datos personales se registrará por el proceso establecido en la legislación. Adicionalmente, las Empresas decidirán las actividades que deben ejecutar al interior de cada una para dar atención conforme a los plazos aplicables, asignar responsabilidades y actividades por responsables, así como la forma de documentar las solicitudes relacionadas con el ejercicio de derechos ARCO.

## **8. Medidas de seguridad**

Las Empresas implementarán las medidas de seguridad técnicas y organizativas necesarias para proteger los datos personales y evitar su alteración, pérdida, tratamiento y/o acceso no autorizado conforme a su política de seguridad de los datos personales.

En este sentido, se cumplirá con la legislación vigente en materia de medidas de seguridad, específicamente elaborar y mantener actualizado un documento de seguridad que contenga lo siguiente:

- Control y registro de accesos y privilegios, así como su verificación periódica.
- Política para la gestión y tratamiento de datos personales.
- Inventario de los datos personales tratados y los sistemas empleados.

Además, deberá establecer políticas para el cumplimiento de las siguientes obligaciones:

- Copias y backup de la información de forma controlada y autorizada.
- Seguridad en los ambientes de procesamiento de datos personales.
- Registro de eventos, interacciones lógicas.
- Identificación y autenticación de usuarios por medio de la gestión y uso de contraseñas.

En general las Empresas y todos sus colaboradores que trabajen con datos personales cumplirán con las medidas de seguridad correspondientes a la naturaleza de la Información objeto de tratamiento.

Las Empresas adoptarán e implementarán una política de seguridad en donde se indiquen, por lo menos, las actividades que se deben ejecutar al interior de la organización ante vulneraciones de datos personales (daño, pérdida, alteración, destrucción o tratamiento no autorizados) y se establezcan los procesos.

## **9. Transferencia de datos personales**

Los datos personales objeto de tratamiento por parte de las Empresas sólo podrán ser cedidos o transferidos a terceros para el cumplimiento de los fines debidamente informados al titular, siempre que cuenten con el consentimiento previo, expreso, libre, inequívoco e informado del titular de los datos personales, salvo cuando sean necesarios para llevar a cabo alguna de las etapas de una relación comercial y/o alguna de las excepciones admitidas por la legislación. En caso que, la transferencia sea necesaria para cumplir la finalidad informada o se encuentre amparada en alguna excepción legal, aun en esos casos subsiste la obligación por parte de las Empresas de informar dicha transferencia al titular del dato personal.

## 10. Encargo del tratamiento

Toda vez que las Empresas encarguen el tratamiento de datos personales de su titularidad – sea que esta información esté o no organizada en un banco de datos - o permitan el acceso de terceros a dicha información para la prestación de algún servicio específico, se deberán tener en cuenta las siguientes especificaciones:

- Todo tratamiento de datos personales realizado por un tercero distinto a las Empresas deberá estar regulado en un contrato, estableciéndose expresamente que el tratamiento de los datos personales se realizará siguiendo las instrucciones de las Empresas y, que únicamente se tratarán los datos personales para los fines autorizados o establecidos en el contrato, por lo que el encargado no los utilizará con una finalidad distinta, ni los comunicará indebidamente a otras personas.
- Todo tercero encargado del tratamiento deberá cumplir con los requisitos establecidos en la legislación.
- El contrato deberá estipular las medidas de seguridad que el encargado del tratamiento está obligado a implementar, tales como la devolución o destrucción de los datos personales una vez finalizado el encargo.
- El contrato deberá establecer que en caso de incumplimiento el infractor responderá ante el titular y ante las autoridades por todo tratamiento o uso no autorizado de los datos personales.
- Si el encargado del tratamiento necesita subcontratar con terceros para brindar parte de los servicios que se obligó a ofrecer, deberá contar con la autorización previa de Intercorp y ésta sólo procederá siempre que el subcontratista asuma las mismas obligaciones que el encargado del tratamiento.
- El contrato deberá establecer además obligaciones de confidencialidad respecto a los datos personales a la que accede el encargado del tratamiento, manteniéndose dichas obligaciones en vigor aún después de finalizado el plazo de vigencia del contrato.
- Para el caso de que cualquier otro tercero trate datos personales respecto de los que las Empresas debe realizar un tratamiento lícito, dicho tercero también deberá realizar el tratamiento conforme a los principios, deberes y obligaciones contenidos en la normatividad vigente en materia de protección de datos personales.

- En caso el titular del dato presentase una solicitud del ejercicio del derecho ante el encargado de tratamiento de los mismos o tercero, este deberá trasladarlo en un plazo máximo de tres (3) días al titular del banco de datos o responsable del tratamiento a fin de que se atienda la solicitud correspondiente.

## 11. Incidentes de seguridad

En caso algún colaborador de las Empresas, así como cualquier tercero que tenga acceso o realice tratamiento de datos personales detecte un Incidente de Seguridad de datos personales (brecha de seguridad, incidente, incumplimiento o afectación a las disposiciones de esta política, o incluso riesgo de su configuración, indicio o entre otros), tendrá la obligación de comunicarlo de forma escrita al Oficial de Datos Personales o al área de legales de las Empresas de forma inmediata. Estos incidentes serán atendidos conforme a los lineamientos específicos de las Empresas, conforme a los procedimientos y obligaciones previstas en la legislación, que incluyen, entre otras cosas, el reporte, cuando corresponda, del Incidente de Seguridad de datos personales a la Autoridad Nacional de Datos Personales del MINJUS.

## 12. Responsabilidades

Esta Política es aprobada por la Gerencia General de Intercorp y distribuida a todos los Gerentes Generales (o sus equivalentes) de las Empresas; quienes deberán asegurar la aprobación de los órganos de gobierno competentes y su difusión e implementación, en coordinación con el Oficial de Datos de las Empresas.

Adicionalmente, existen las siguientes obligaciones aplicables a los órganos o funcionarios que se detallan a continuación:

### 12.1. Directorio de cada Empresa

- Aprobar y supervisar el cumplimiento de la presente Política
- Ejercer una supervisión razonable del cumplimiento de la presente Política.

### 12.2. Gerente General de cada Empresa

- Asegurar el cumplimiento y la ejecución de lo establecido en la presente Política.
- Autorizar la adecuada provisión de recursos financieros, tecnológicos y humanos para implementar y mantener lo establecido en la presente Política.
- Aprobar la política de sanciones por los incumplimientos relacionados con la presente Política.
- Designar al Oficial de Datos Personales, quien será el responsable de la implementación y supervisión de la presente Política.

### 12.3 Responsable de Integridad y Cumplimiento de cada Empresa



- Supervisar y coordinar el adecuado cumplimiento, ejecución e implementación de lo establecido en la presente Política.

#### **12.4 Oficial de Datos Personales**

- Las señaladas en el artículo 37 y siguientes del Decreto Supremo No. 016-2024-JUS.
- Coordinar y monitorear las actividades para la implementación, el adecuado desarrollo, y cumplimiento de lo establecido en la presente Política.
- Proporcionar asesoramiento y orientación al Encargado de Protección de Datos Personales en la gestión e implementación de la presente Política.
- Entre sus responsabilidades se debe considerar las siguientes:
  - Inscribir los Bancos de Datos Personales y mantenerlos actualizados ante la Autoridad Nacional competente.
  - Inscribir la transferencia de información transfronteriza.
  - Adaptar la Política de Protección de Datos Personales a la Empresa en particular de acuerdo a la naturaleza e industria, a los objetivos estratégicos del negocio, la legislación y la normativa vigente y coordinar su publicación y difusión.
  - Definir los encargados de los Bancos / Sub Bancos de Datos que gestiona cada Empresa.
  - Proporcionar la información relativa al tratamiento de datos personales a la Autoridad Nacional de Protección de Datos Personales cuando esta lo requiera, así mismo permitirle el acceso a los bancos de datos personales que cada Empresa administra.
  - Guardar toda la información respecto a la solicitud de los derechos ARCO en medios físicos o digitales.
  - Coordinar el cumplimiento e implementación de los controles de seguridad necesarios, en coordinación con las áreas de negocio y tecnología, definidos en la presente política.
  - Revisar periódicamente la efectividad de los controles de seguridad adoptados para la protección de los bancos de datos personales y generar acciones de mejora.

#### **12.5 Directores y colaboradores**

- Cumplir con los lineamientos de la presente Política.
- Buscar orientación en caso tengan alguna duda respecto a la aplicación de la presente Política.
- Reportar, a través de los canales dispuestos para este fin, cualquier incumplimiento a la presente Política.

### **13. Lineamientos Generales para los responsables del tratamiento de datos personales**

- Las Empresas cumplirán con lo dispuesto en el marco normativo vigente en materia de protección de datos personales y seguridad de la información en los lugares en donde realicen actividades empresariales.
- En caso la legislación local de algunas de las Empresas, considere mayores restricciones o actividades a las planteadas, se deben aplicar las más exigentes para cada Empresa.
- Las Empresas estarán sujetas a los lineamientos que puedan establecer sus reguladores o al interno, de manera independiente, de acuerdo al giro de negocio o con las actividades empresariales que realicen.
- Las Empresas gestionarán la implementación de actividades para la evaluación y monitoreo continuo de los controles y señales de alerta diseñados para el adecuado tratamiento de datos personales de nuestros grupos de interés.
- Los directores y colaboradores deberán comprometerse a proteger y no permitir el acceso a datos personales a personas que no hayan sido autorizadas, garantizando el derecho de privacidad en el tratamiento de los datos personales recopilados, así como de su seguridad a través de medidas técnicas, organizativas y legales que eviten la alteración, pérdida, tratamiento o acceso no autorizado.
- Las Empresas no podrán revelar datos personales a terceros sin autorización expresa del titular del dato, salvo que sea ordenado por mandato de un juez u organismo del gobierno en el ámbito de sus competencias (ej. Superintendencia Nacional de Administración Tributaria (SUNAT), Congreso de la República, Unidad de Inteligencia Financiera (UIF), entre otras excepciones establecidas en la ley de la materia, con las garantías previstas en la Ley.
- Cualquier duda y/o inquietud relacionada con el cumplimiento de la presente Política deberá ser canalizada al Oficial de Datos Personales y comunicada a través de los canales disponibles.
- Las Empresas deberán realizar capacitaciones con el fin de sensibilizar a los directores y colaboradores sobre la importancia de una adecuada gestión de los datos personales e información confidencial, las cuales deberán ser debidamente documentadas.
- Es importante que los principios y valores del Grupo Intercorp, incluyendo Nuestro Compromiso con la Integridad, el Sistema Corporativo de Integridad y Cumplimiento, así como la presente Política prevalezcan en cualquier situación.

#### **14. Lineamientos Específicos para los responsables del tratamiento de datos personales**

Estos son los lineamientos mínimos que deberán ser cumplidos por todos los directores, colaboradores y socios de negocio para salvaguardar los Datos Personales y Datos Sensibles:

- Se podrán recopilar datos personales únicamente para fines específicos y se limitará a la necesidad para la cual se está recopilando la información.
- Las Empresas deberán obtener el consentimiento previo e informado de los titulares de datos personales antes de tratar sus datos personales salvo cuando sean necesarios para llevar a cabo alguna de las etapas de una relación contractual y/o alguna de las excepciones admitidas por la legislación.

- Los datos personales, al igual que toda información recopilada, serán utilizados exclusivamente para los fines determinados, los cuales deberán ser claros y lícitos.
- Los datos personales recopilados deberán ser proporcionales y no excesivos a la finalidad para la que estos hayan sido recopilados. Cualquier otra actividad que se realice con dichos datos deberá ser autorizada por los titulares de los datos en uso.
- El consentimiento para el tratamiento de datos personales, especialmente, en el caso de datos sensibles debe ser explícito y otorgado a través de los medios permitidos por la normativa aplicable y disposiciones normativas.
- El titular de los datos personales tendrá el derecho de revocar su consentimiento cuando lo desee y sin necesidad de brindar alguna justificación, a menos que el uso de sus datos personales esté amparado por la normativa aplicable debido a la relación que ostenta con la Empresa que corresponda. En dichos casos, la revocación ocurrirá una vez terminada la relación correspondiente. Cualquier caso excepcional deberá ser evaluado y autorizado por las instancias correspondientes y la Gerencia Legal de la Empresa.
- En caso de tratar con datos personales de un menor de edad, se requerirá del consentimiento de sus padres o tutores.
- Los datos personales almacenados en las bases de datos de las Empresas serán considerados información confidencial, y solo podrán ser accedidos, transferidos y utilizados para los fines establecidos.
- Las Empresas deberán tomar medidas específicas y razonables para asegurar la debida conservación de la información bajo las condiciones de seguridad, de modo que se pueda evitar la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Las Empresas son responsables de contar con controles específicos para verificar que la información de los bancos de datos a ser registrados sea completa, exacta, se encuentre actualizada, sea comprensible y comprobable.
- Se establecerán controles de seguridad que sean necesarios para el flujo transfronterizo de datos personales, con la finalidad de asegurar el cumplimiento de la normativa aplicable. Dichos controles, deberán ser determinados tomando en cuenta el país destinatario y los listados elaborados al respecto por la Autoridad Nacional de Datos Personales del MINJUS, giro del negocio, la cantidad de personas que tienen acceso a los datos, los niveles de autorización y supervisión, entre otros.
- Salvo por las excepciones establecidas por la normativa aplicable y disposiciones normativas, las transferencias de datos personales deberán contar siempre con el consentimiento de los titulares y deberán seguir la política de seguridad de la información vigente.
- Se rectificará, actualizará o incluirá mayor detalle de los datos personales cuando se advierta omisión, error, o falsedad en los mismos. Toda rectificación de datos personales deberá ser justificada a través de documentación apropiada.
- Las Empresas podrán transferir datos personales a entidades públicas legalmente facultadas dentro del ámbito de sus funciones cuando así sea dispuesto por la legislación aplicable, o por orden o requerimiento de una entidad autorizada.
- Se suprimirán los datos personales cuando estos hayan dejado de ser necesarios, cuando se haya agotado la finalidad para la cual fueron recopilados, o cuando se haya vencido la vigencia del plazo establecido, de acuerdo a Ley.
- Los titulares de los datos personales pueden oponerse al tratamiento de sus datos personales en cualquier momento, lo cual será respetado por las

- Empresas, siempre y cuando, no se trate de información que cuente con una debida justificación contractual o legal para realizar el tratamiento.
- Las Empresas deberán establecer procedimientos simples para el ejercicio de los derechos del titular de los Datos Personales (ARCO), considerando canales adecuados de atención adecuados, tramitación de solicitudes dentro de los plazos establecidos en la normativa.

## 15. Monitoreo y Auditoría

A nivel corporativo, el monitoreo del cumplimiento de esta y otras políticas del Grupo está a cargo del Comité de Integridad Corporativo. A nivel Empresa, será el Oficial de Datos Personales y/o la persona designada de manera interna quien vele por dicho cumplimiento.

Las áreas de Auditoría Interna o Control Interno de cada Empresa ejecutarán las revisiones periódicas de las operaciones clave de la Empresa para asegurar el cumplimiento continuo del Programa de Integridad y Cumplimiento y de los lineamientos estipulados en la presente política.

Tomamos acción ante cualquier falta realizada en perjuicio de nuestros directores, colaboradores y socios de negocio, asegurando las medidas necesarias para resolver cualquier tipo de incumplimiento o conflicto referente a la presente política o al Sistema Corporativo de Integridad y Cumplimiento.

## 16. Canales de Comunicación

Cualquier irregularidad o inconsistencia con la presente Política deberá ser reportada a través de los canales de denuncia disponibles. Ante cualquier duda o consulta, el colaborador podrá acudir al Oficial de Datos Personales, a su superior inmediato, al Responsable de Integridad y Cumplimiento de la Empresa, a la Gerencia Legal de la misma o a alguna autoridad competente dentro del Sistema Corporativo de Integridad y Cumplimiento.

## 17. Sanciones por Incumplimientos

El incumplimiento de los lineamientos establecidos en la presente Política corporativa y en las políticas relacionadas al Sistema Corporativo de Integridad y Cumplimiento estarán sujetos a las medidas disciplinarias pertinentes, las cuales serán designadas por el Comité de Integridad Corporativo, el Comité de Integridad de Plataforma o el Comité de Integridad de la Empresa (según se requiera).

Asimismo, dichos incumplimientos podrían suponer infracciones a las leyes aplicables, por lo que los responsables podrían ser sujetos a acciones civiles o penales por parte de las autoridades competentes



## **18. Vigencia**

Esta política ha sido aprobada mediante decisión adoptada por Intercorp, el día 26 de Marzo de 2025