Normativa de Protección de Datos Personales

INTEGRATEL PERÚ S.A.A.

Edición 1- Marzo 2026

Índice

Contenido

1. Introducción 5
2. Objeto 5
3. Ámbito de aplicación 5
4. Contenido 6
4.1. Definiciones 6
4.2. Disposiciones para el cumplimiento de los Principios 8
4.2.1. Determinación previa de la finalidad y proporcionalidad 8
4.2.2. Base legal del Tratamiento y gestión del Consentimiento 8
4.2.3. Transparencia y deber de información 9
4.2.4. Calidad y actualización de Datos Personales 9
4.2.5 Conservación, eliminación y anonimización 9
4.2.6. Garantía de nivel adecuado de protección 10
4.2.7. Garantía del ejercicio de derechos del Titular del Dato 10
4.2.8. Responsabilidad proactiva y documentación 10
4.3. Gobierno del Dato 10
4.3.1. Gestión de Bancos de Datos Personales 11
4.3.2. Inventario de Tratamientos 11
4.3.3. Inventario de Activos 12
4.3.4 Evaluaciones de Impacto 12
4.4. Medidas de Seguridad 12
4.4.1. Medidas técnicas 13
4.4.2. Medidas organizativas 13
4.4.3. Eliminación y destrucción segura 13

4.5. Gestión de Incidentes de Seguridad 13
4.5.1 Reporte inmediato interno 13
4.5.2. Evaluación y clasificación 14
4.5.3. Medidas de contención y mitigación 14
4.5.4. Notificación a la Autoridad 14
4.5.5. Comunicación a los Titulares 14
4.5.6 Registro de Incidentes de Seguridad 15
4.6. Relación con Proveedores y cadena de suministro 15
4.6.1. Encargos de Tratamiento 15
4.6.2. Evaluación y selección de Proveedores 15
4.6.3. Sub-encargados 16
4.6.4. Monitoreo y supervisión 16
4.6.5. Supresión o devolución al término del contrato 16
4.6.6. Transferencias internacionales 16
4.7. Modelo de Gobernanza y responsabilidades 16
4.7.1. Gerencia General y Comité de Dirección 17
4.7.2. Oficial de Datos Personales (DPO) 17
4.7.3. Responsable Interno del Tratamiento 17
4.7.4. Área de Seguridad 17
4.8. Responsabilidades operativas de las áreas 18
4.8.2. Área Legal y Regulación 18
4.8.3. Área de Personas 18
4.8.4. Auditoría Interna 19
4.9. Obligaciones individuales 19
4.9.1. Obligaciones de los Trabajadores 19
4.9.2. Obligaciones de los Proveedores 19
4.10. Consecuencias del incumplimiento 20

4.10.1. Para Trabajadores 20

4.10.2. Para Proveedores 20

5. Entrada en vigor 20

6. Anexos 21

7. Anexo 1: Política de Privacidad para Trabajadores de Integratel..... 22

8. Anexo 2: Cláusula de protección de Datos Personales – Contratos Laborales..... 25

9. Anexo 3: Política de Privacidad de Clientes..... 26

10. Anexo 4: Cláusulas en contratos de abonados (Clientes).....29

11. Anexo 5: Formato ARCO..... 30

12. Anexo 6: Política de Cookies.....31

13. Anexo 7: Contrato de Encargo de Tratamiento de Datos Personales – DPA.....32

14. Anexo 8: Declaración Jurada: Devolución/Supresión de la Información.....58

Versión	Responsable	Fecha	Aprobación Directorio
1	Gerencia de Regulación y Asuntos Públicos	Marzo 2026	Marzo 2026

1. Introducción

Integratel Perú S.A.A. (en adelante, "Integratel" o "La Compañía") aprueba la presente Normativa de Protección de Datos Personales, la cual constituye su Código de Conducta en materia de protección de Datos Personales, en concordancia con la Ley N° 29733[1], su Reglamento aprobado por Decreto Supremo N° 016-2024-JUS y demás disposiciones aplicables (en adelante, la Legislación Vigente).

En su condición de Código de Conducta, la presente Normativa establece el marco interno que regula el Tratamiento de Datos Personales bajo responsabilidad de la Compañía, asegurando la implementación práctica y efectiva de los principios y obligaciones previstos en la Legislación Vigente.

2. Objeto

La presente Normativa tiene por objeto desarrollar y complementar la Política de Protección de Datos Personales de Integratel, estableciendo disposiciones internas, reglas operativas, mecanismos de control y responsabilidades específicas que permitan garantizar el cumplimiento efectivo de la normativa en materia de protección de Datos Personales.

Asimismo, busca prevenir riesgos legales, económicos y reputacionales derivados del Tratamiento indebido de Datos Personales, promoviendo una cultura organizacional basada en la diligencia, confidencialidad y gestión basada en riesgos.

3. Ámbito de aplicación

La presente Normativa es de cumplimiento obligatorio para miembros del Directorio y Gerencia General, Trabajadores, Proveedores o Encargados de Tratamiento de Datos Personales que actúen en nombre o por cuenta de Integratel.

Es aplicable a todo Tratamiento de Datos Personales realizado bajo responsabilidad de la Compañía, cualquiera sea el medio, soporte o tecnología utilizada.

La presente Normativa deberá interpretarse y aplicarse de manera sistemática y complementaria con la Política de Protección de Datos Personales, los Lineamientos de Seguridad para el Tratamiento de Datos Personales[2], y demás documentos internos vinculados.

En caso de discrepancia, prevalecerá la disposición que otorgue mayor nivel de protección a los Datos Personales.

[1] Ley de Protección de Datos Personales.
[2] Equivale al Documento de Seguridad establecido en el artículo 47 del Reglamento de la Ley de Protección de Datos Personales aprobado mediante Decreto Supremo N° 016-2024-JUS.

4. Contenido

4.1. Definiciones

a) Anonimización
Procedimiento en virtud del cual se realiza un Tratamiento de Datos Personales con fines de impedir la identificación del titular de los Datos Personales. Es irreversible.

b) Autoridad Nacional de Protección de Datos Personales
Entidad encargada de realizar las acciones necesarias para el cumplimiento de la Legislación Vigente, ejerciendo funciones fiscalizadoras y sancionadoras. En adelante, "La Autoridad" o la "ANPDP".

c) Banco de Datos Personales
Conjunto organizado de Datos Personales, automatizado o no, independientemente del soporte o formato, que permite su acceso, Tratamiento o recuperación. En adelante, "El Banco" o "Los Bancos".

d) Consentimiento
Manifestación de voluntad libre, previa, expresa e informada mediante la cual el titular de los Datos Personales autoriza el Tratamiento de sus datos para una finalidad determinada, conforme a la Legislación Vigente.

e) Consejo Nacional de Seguridad Digital
Organismo que gestiona, dirige y supervisa la seguridad digital del país como parte de la seguridad nacional[3].

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. Ejemplos: la información del cliente en el sistema comercial como nombres, apellidos, dirección, número de teléfono, IMEI, IMSI, documento de identidad, facturación, entre otros.

g) Datos Personales Sensibles
Aquellos Datos Personales que dada su naturaleza requieren un cuidado especial, de acuerdo con la Legislación Vigente. Ejemplos: datos biométricos, ingresos económicos, opiniones políticas, o morales, afiliación sindical, e información vinculada a salud.

h) Derechos ARCO
Conjunto de derechos que asisten al Titular de Datos Personales para acceder, rectificar, cancelar o suprimir y oponerse al Tratamiento de sus Datos Personales.

i) Disociación
Procedimiento en virtud del cual se realiza un Tratamiento de Datos Personales con fines de impedir la identificación del Titular de los mismos o de un atributo o cualidad de él que lo haga identificable, mientras se mantiene cierto nivel de información sobre el mismo. Es reversible.

[3] Se crea mediante el D.U. N° 007-2020 que aprueba el Marco de Confianza Digital.

j) DPA[4]
Es el Contrato de Encargo de Tratamiento de Datos Personales que debe suscribirse y acompañarse como anexo del contrato principal con Proveedores, siempre que se comparta Datos Personales para un Tratamiento de Datos Personales por encargo de Integratel**.**

k) DPO[5]
Es el Oficial de Datos Personales, encargado de verificar e informar el cumplimiento de la presente Normativa.

l) Encargado del Tratamiento de Datos Personales
Es el Proveedor que realiza el Tratamiento de los Datos Personales, por encargo de Integratel, en virtud de una relación contractual que delimita el ámbito de su actuación. Todo Encargado del Tratamiento de Datos Personales debe suscribir con el Responsable un DPA. En adelante el "Encargado" o el "Proveedor".

m) Flujo Transfronterizo o Transferencia Internacional de Datos Personales
Transferencia 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.

n) Incidente de Seguridad
Es 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.

o) Registro lógico o LOG
Archivo que registra sistemáticamente los eventos o acciones que ocurren en un sistema o aplicación. Deberá permitir la trazabilidad de la interacción lógica.

p) Responsable del Tratamiento de Datos Personales
Es la persona jurídica que decide sobre la finalidad y medios del Tratamiento de Datos Personales. Para efectos de la presente Normativa, Integratel es la Responsable del Tratamiento de Datos Personales, salvo situaciones que establezcan lo contrario. En adelante, el "Responsable".

q) Responsable Interno del Tratamiento de Datos Personales
Área, función o rol designado dentro de Integratel que determina la finalidad y alcance de uno o más Tratamientos de Datos Personales en el ámbito de su competencia. Es responsable de asegurar la implementación efectiva de las disposiciones establecidas en la presente Normativa respecto de los Tratamientos bajo su ámbito, en coordinación con el DPO y Seguridad. En adelante, el "Responsable Interno".

r) Titular(es) de Datos Personales
Persona natural a quien corresponden los Datos Personales materia de Tratamiento**.** Las personas jurídicas no son sujeto de derechos al amparo de la Legislación Vigente.

s) Transferencia de Datos Personales
Toda transmisión de Datos Personales a una persona distinta del Titular de los Datos Personales.

[4] Por sus siglas en inglés *"Data Protection Agreement"*.
[5] Por sus siglas en inglés *"Data Protection Officer"*.

t) Tratamiento de Datos Personales
Cualquier operación o conjunto de operaciones automatizados o no, que se realicen sobre los Datos Personales. Se incluye la recopilación, registro, organización, almacenamiento, conservación, modificación, consulta, explotación, extracción y/o cualquier otro procedimiento en general que facilite el acceso, correlación o interconexión de los Datos Personales. (En adelante, "Tratamiento").

4.2. Disposiciones para el cumplimiento de los Principios

Las siguientes disposiciones desarrollan los mecanismos internos destinados a asegurar la aplicación efectiva de los Principios establecidos en la Política de Protección de Datos Personales, mediante la definición de reglas claras de actuación, responsabilidades y controles, a fin de garantizar un Tratamiento adecuado, transparente y alineado con la Legislación Vigente.

4.2.1. Determinación previa de la finalidad y proporcionalidad

Antes de iniciar cualquier Tratamiento, el Responsable Interno deberá:

- Definir de manera expresa la finalidad específica del Tratamiento.
- Verificar que los Datos Personales a recolectar sean estrictamente necesarios para dicha finalidad.
- Evitar la recolección de Datos Personales "por si acaso" o sin justificación operativa clara.

Cuando exista duda sobre la proporcionalidad o legitimidad del Tratamiento, el Responsable Interno deberá consultar previamente al DPO.

4.2.2. Base legal del Tratamiento y gestión del Consentimiento

Para poder tratar Datos Personales debemos contar con una justificación legal conforme a la Legislación Vigente. La regla general es que el Tratamiento requiere el consentimiento del Titular, salvo excepción expresa prevista en la Legislación Vigente.

Cuando necesitamos Consentimiento

Si el Tratamiento se basa en el Consentimiento:

- Debe obtenerse antes de tratar los Datos Personales.
- El Titular debe estar claramente informado.
- Debe quedar evidencia de que aceptó (registro físico o digital).
- El Titular debe poder retirar el Consentimiento cuando corresponda.

Ejemplo: enviar ofertas comerciales o realizar llamadas promocionales, requiere Consentimiento.

En el caso de Datos Sensibles (como datos biométricos, datos de remuneración u otros datos especialmente protegidos), el Consentimiento debe garantizar de manera inequívoca la voluntad del titular de los datos.

El DPO verificará que los mecanismos utilizados para obtener y registrar el Consentimiento cumplan con la Legislación Vigente.

Cuando no se necesita consentimiento

No será necesario solicitar Consentimiento cuando la Legislación Vigente lo permita expresamente.

En Integratel, esto ocurre principalmente en los siguientes casos:

- Cuando el Tratamiento es necesario para la ejecución de un contrato. Ejemplo: enviar recibos, gestionar pagos o brindar el servicio contratado.
- Cuando una entidad pública solicita información en ejercicio de sus funciones legales. Ejemplo: requerimientos de OSIPTEL.

Si existe duda sobre si corresponde o no solicitar Consentimiento, debe consultarse previamente con el DPO.

4.2.3. Transparencia y deber de información

Todo Tratamiento de Datos Personales deberá cumplir previamente con el deber de información al Titular, el cual deberá brindarse de manera clara, sencilla, accesible y comprensible, conforme a la Legislación Vigente.

Cuando los Datos Personales sean proporcionados directamente por el Titular, el deber de información podrá cumplirse, entre otros mecanismos, mediante:

- La Política de Privacidad aplicable.
- Cláusulas informativas específicas según el canal de recolección.
- Avisos en entornos digitales.
- Comunicación verbal debidamente sustentada cuando el canal así lo permita.
- Cualquier otro medio idóneo que garantice que el Titular ha sido informado antes del Tratamiento.

En los supuestos en que los Datos Personales no sean obtenidos directamente del Titular, Integratel adoptará las medidas necesarias para cumplir con el deber de información en las condiciones previstas en la Legislación Vigente.

Toda campaña comercial, nueva herramienta tecnológica o canal de captación deberá ser revisado previamente por el DPO para asegurar el cumplimiento del deber de información.

4.2.4. Calidad y actualización de Datos Personales

Los Responsables Internos deberán adoptar medidas razonables para:

- Mantener los Datos Personales actualizados.
- Corregir información inexacta cuando sea advertida.
- Eliminar o bloquear Datos Personales que hayan perdido pertinencia.

4.2.5 Conservación, eliminación y anonimización

Los Datos Personales solo podrán conservarse durante el plazo necesario para cumplir la finalidad que motivó su recolección, salvo obligación legal distinta. Cumplida la finalidad:

- Deberán eliminarse de manera segura.
- O anonimizarse cuando corresponda.
- O bloquearse si existe obligación legal de conservación.

La eliminación deberá realizarse bajo procedimientos técnicos que impidan su recuperación no autorizada.

4.2.6. Garantía de nivel adecuado de protección

Integratel deberá asegurar que todo Tratamiento, incluyendo aquellos realizados por Encargados fuera del Perú, mantenga un nivel de protección equivalente al exigido por la Legislación Vigente. Para tal efecto:

- Todo Proveedor que trate Datos Personales en nombre de Integratel deberá suscribir un DPA.
- Cuando el Tratamiento involucre flujo transfronterizo a un país sin nivel adecuado[6] de protección adecuado, deberá suscribirse adicionalmente un Acuerdo de Transferencia (integrante del DPA).
- Integratel verificará periódicamente las medidas de seguridad que aplica el Encargado a los Datos Personales materia del encargo.

4.2.7. Garantía del ejercicio de derechos del Titular del Dato

Integratel adoptará las medidas necesarias para garantizar el ejercicio efectivo de los derechos reconocidos por la Legislación Vigente, conocidos como Derechos ARCO. Estos incluyen a los derechos de información, acceso, rectificación, cancelación y oposición. Para tal efecto:

- Se habilitarán e informarán canales adecuados y accesibles.
- Las solicitudes deberán ser registradas y atendidas dentro de los plazos legales.
- Toda respuesta deberá estar debidamente fundamentada cuando corresponda.
- Integratel conservará los documentos que evidencien la oportuna atención a las solicitudes presentadas, tanto las que fueron aprobadas como denegadas.
- Cuando resulte técnica y jurídicamente procedente, Integratel facilitará el ejercicio del derecho de portabilidad del dato en formatos estructurados y de uso común.

4.2.8. Responsabilidad proactiva y documentación

Integratel adopta el principio de responsabilidad proactiva como eje transversal de la presente Normativa. En virtud de ello, la Compañía deberá:

- Mantener evidencia documentada de sus decisiones en materia de protección de Datos Personales.
- Conservar registros de Consentimiento, y Evaluaciones de Impacto relativas a la protección de Datos Personales.
- Mantener inventarios actualizados de Tratamientos y Activos.
- Documentar la gestión de Incidentes de Seguridad y las medidas correctivas adoptadas.
- Evaluar periódicamente la eficacia de sus controles internos.

.

4.3. Gobierno del Dato

Integratel adopta un enfoque de gestión de Datos Personales basado en el análisis y mitigación de riesgos, considerando la naturaleza, alcance, contexto y finalidad de cada Tratamiento.

Las medidas técnicas, organizativas y legales implementadas deberán ser proporcionales al nivel de riesgo que el Tratamiento pueda generar sobre los derechos de los Titulares. Para ello:

[6] Ver lista de países con nivel de protección adecuado aquí: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

- Todo Tratamiento deberá ser evaluado previamente desde una perspectiva de riesgo.
- Se prestará especial atención al Tratamiento de Datos Personales Sensibles, al perfilamiento automatizado, al uso de nuevas tecnologías y a las transferencias internacionales.
- El DPO determinará cuándo corresponde realizar una Evaluación de Impacto relativa a la protección de Datos Personales.
- Las medidas de control no serán uniformes para todos los Tratamientos, sino que se ajustarán al nivel de riesgo identificado.

4.3.1. Gestión de Bancos de Datos Personales

Integratel debe identificar y, documentar los conjuntos de Datos Personales que se generen o utilicen en el marco de sus actividades, cualquiera sea su soporte (físico, digital o tecnológico), a fin de que el DPO pueda evaluar si corresponde su inscripción, modificación o cancelación ante la Autoridad[7].

Cada Responsable Interno tiene la obligación de:

- Informar al DPO la creación, modificación o eliminación de conjuntos de Datos Personales dentro de su área.
- Remitir información completa y veraz sobre la finalidad, categorías de datos personales, destinatarios, medidas de seguridad y demás aspectos relevantes.
- Validar que la información que se inscriba o actualice ante la Autoridad, sea exacta y refleje fielmente la realidad del Tratamiento efectuado.
- No implementar nuevos Tratamientos ni modificar sustancialmente los existentes sin comunicarlo previamente al DPO.
- La omisión de estas obligaciones constituye un incumplimiento de la Legislación Vigente y puede generar sanciones administrativas para Integratel.

4.3.2. Inventario de Tratamientos

Integratel mantendrá un inventario interno de Tratamientos de Datos Personales que constituye su Registro de Actividades de Tratamiento. El DPO será responsable de la administración y consolidación del Inventario, sobre la base de la información proporcionada por los Responsables Internos.

El Inventario incluirá, como mínimo:

- Finalidad del Tratamiento.
- Categoría de Datos Personales tratados.
- Categorías de Titulares.
- Base legal que sustenta el Tratamiento.
- Plazos de conservación.
- Encargados y Sub - encargados autorizados.
- Flujos Transfronterizos, de ser el caso.
- Medidas técnicas y organizativas de seguridad implementadas.

[7] Registro Nacional de Protección de Datos Personales.

Cada Responsable Interno deberá:

- Informar oportunamente al DPO cualquier creación, modificación o eliminación de un Tratamiento.
- Actualizar la información correspondiente a su área cuando se produzcan cambios relevantes.
- Revisar, al menos de manera anual, la información vinculada a los Tratamientos bajo su responsabilidad.

El incumplimiento de esta obligación podrá generar responsabilidades conforme a la Legislación Vigente y a las disposiciones internas aplicables.

4.3.3. Inventario de Activos

El área de TI deberá mantener actualizado el inventario de Activos, entendidos como todo sistema que soporte los Tratamientos de Datos Personales al interior de Integratel.

Este inventario permitirá, entre otros:

- Identificar los Datos Personales tratados, precisando si existen Datos Sensibles.
- Identificar riesgos.
- Gestionar accesos.
- Controlar integraciones.
- Planificar medidas de seguridad en coordinación con Seguridad.

La actualización del inventario deberá realizarse de forma periódica o cuando se implementen nuevos sistemas, e informarlo previamente al DPO.

4.3.4 Evaluaciones de Impacto

Cuando un Tratamiento pueda implicar alto riesgo para los derechos de los Titulares, deberá realizarse una Evaluación de Impacto relativa a la protección de Datos Personales. Se considerarán, entre otros, los siguientes supuestos:

- Tratamiento de Datos Personales Sensibles.
- Uso de tecnologías emergentes o inteligencia artificial.
- Creación de perfiles personales.
- Monitoreo sistemático de personas.

Toda Evaluación de Impacto relativa a la protección de Datos Personales deberá documentarse y conservarse como evidencia de cumplimiento.

4.4. Medidas de Seguridad

Integratel implementará medidas técnicas y organizativas apropiadas para proteger los Datos Personales contra la pérdida, alteración, acceso no autorizado, uso indebido o cualquier Tratamiento contrario a la Legislación Vigente.

Dichas medidas serán proporcionales al riesgo identificado, considerando la naturaleza de los Datos Personales, el alcance del Tratamiento, el contexto operativo y las posibles afectaciones a los derechos de los Titulares.

Las medidas adoptadas estarán documentadas en los Lineamientos de Seguridad para el Tratamiento de Datos Personales y en los procedimientos internos correspondientes que elabore el área de Seguridad.

4.4.1. Medidas técnicas

Podrán incluir, según el riesgo identificado:

- Autenticación robusta y mecanismos MFA.
- Control y registro de accesos (logs).
- Conservación de logs por un período de 02 años.
- Sistemas de prevención de fuga de información.
- Cifrado cuando corresponda.
- Pseudonimización o anonimización.
- Monitoreo continuo de accesos y actividades inusuales.

Las medidas no constituyen una lista taxativa y podrán ampliarse conforme evolucione el riesgo tecnológico.

4.4.2. Medidas organizativas

Integratel deberá implementar, entre otras:

- Asignación de roles y responsabilidades claras.
- Segregación de funciones.
- Gestión de accesos basada en el principio de mínimo privilegio.
- Capacitación periódica obligatoria.
- Procedimientos documentados de gestión de Datos Personales.

4.4.3. Eliminación y destrucción segura

La eliminación de Datos Personales deberá realizarse mediante procedimientos que impidan su recuperación no autorizada. La destrucción de soportes físicos deberá documentarse cuando el riesgo lo amerite.

4.5. Gestión de Incidentes de Seguridad

Las siguientes disposiciones establecen el procedimiento interno para la identificación, reporte, evaluación y gestión de incidentes de seguridad que involucren Datos Personales, a fin de mitigar riesgos, proteger los derechos de los Titulares y asegurar el cumplimiento de la Legislación Vigente.

4.5.1 Reporte inmediato interno

Todo trabajador, Proveedor o tercero que tome conocimiento de la ocurrencia o sospecha razonable de un Incidente de Seguridad que involucre Datos Personales deberá reportarlo de manera inmediata al área de Seguridad y al DPO, utilizando los canales internos establecidos.

El reporte deberá realizarse aun cuando no se cuente con toda la información disponible, a fin de permitir la evaluación temprana del evento y la adopción oportuna de medidas de contención.

La omisión del reporte inmediato constituye incumplimiento de la presente Normativa y podrá dar lugar a las medidas disciplinarias o contractuales correspondientes.

4.5.2. Evaluación y clasificación

Una vez reportado el Incidente de Seguridad:

- El área de Seguridad evaluará su naturaleza técnica.
- El DPO evaluará su impacto legal y regulatorio.
- Se determinará el nivel de riesgo para los titulares.
- Se documentarán los hechos, medidas adoptadas y decisiones.

4.5.3. Medidas de contención y mitigación

Desde el momento en que se tome conocimiento del incidente, se adoptarán medidas inmediatas para:

- Contener el evento.
- Mitigar posibles efectos adversos.
- Evitar su reiteración.

4.5.4. Notificación a la Autoridad

Cuando el Incidente de Seguridad represente un riesgo relevante para los derechos de los Titulares conforme a los supuestos previstos en la Legislación Vigente, el DPO notificará el incidente ocurrido ante la Autoridad Nacional de Protección de Datos Personales y al Consejo Nacional de Seguridad Digital.

La decisión de notificar será adoptada por el DPO, en coordinación con el Área de Seguridad y el área involucrada, sobre la base de la evaluación del riesgo y del impacto del Incidente de Seguridad.

Previamente a la comunicación externa, se deberá informar a la Gerencia General y al Área de Comunicaciones, a fin de asegurar la adecuada gestión institucional, reputacional y comunicacional del Incidente de Seguridad.

La decisión deberá estar debidamente documentada.

4.5.5. Comunicación a los Titulares

Cuando, como resultado del análisis del incidente, se determine que éste pueda afectar significativamente los derechos de los Titulares de los Datos Personales, Integratel procederá a comunicarlo conforme a lo previsto en la Legislación Vigente.

La decisión de notificar a los Titulares será adoptada por el DPO, en coordinación con el Área de Seguridad de la Información y el área involucrada, sobre la base de la evaluación del riesgo y del impacto del incidente.

Previamente a la comunicación externa, se deberá informar a la Gerencia General y al Área de Comunicaciones, a fin de asegurar la adecuada gestión institucional, reputacional y comunicacional del Incidente de Seguridad. La comunicación a los Titulares deberá incluir, como mínimo:

- Naturaleza del incidente.
- Datos Personales comprometidos.
- Las posibles consecuencias del incidente.
- Medidas adoptadas o propuestas para mitigar sus efectos.
- Recomendaciones pertinentes para protegerse frente a eventuales riesgos.

4.5.6 Registro de Incidentes de Seguridad

Integratel mantendrá un registro centralizado de Incidentes de Seguridad vinculados a Datos Personales, el cual constituirá evidencia de cumplimiento del principio de responsabilidad proactiva.

El Área de Seguridad será responsable de la administración y actualización de dicho registro, en coordinación con el DPO, quien verificará el adecuado análisis legal del Incidente de Seguridad y, cuando corresponda, la gestión de notificaciones a la Autoridad y/o a los Titulares.

Todas las áreas deberán reportar de manera inmediata cualquier Incidente de Seguridad o sospecha de Incidente al Área de Seguridad y al DPO.

4.6. Relación con Proveedores y cadena de suministro

4.6.1. Encargos de Tratamiento

Todo Proveedor que trate Datos Personales por encargo de Integratel deberá suscribir previamente un Contrato de Encargo de Tratamiento de Datos Personales (DPA). El DPA establece como mínimo:

- La finalidad y alcance del Tratamiento.
- Las categorías de Datos Personales materia de Tratamiento.
- La ubicación donde el Encargado alojará los Datos Personales o desde donde accederá a los mismos.
- La duración del encargo.
- Las medidas de seguridad aplicables.
- Las obligaciones de confidencialidad.
- El deber de reporte inmediato de incidentes.
- Las condiciones de sub-contratación.
- La obligación de supresión o devolución al término de la prestación.

Ningún Proveedor podrá iniciar el Tratamiento de Datos Personales sin la suscripción previa del DPA.

4.6.2. Evaluación y selección de Proveedores

Antes de contratar a un Encargado que implique uno o más Tratamientos de Datos Personales, el Responsable Interno deberá:

- Identificar la naturaleza y volumen de los Datos Personales involucrados.
- Evaluar el nivel de riesgo del Tratamiento desde la perspectiva del negocio.
- Informar al DPO y al Área de Seguridad sobre el alcance del Tratamiento propuesto.
- Solicitar la validación correspondiente cuando el Tratamiento pueda implicar riesgos relevantes.

El Área de Seguridad de la Información será responsable de evaluar la suficiencia de las medidas técnicas y organizativas declaradas por el Proveedor.

Cuando el Tratamiento implique riesgos elevados, se requerirá validación previa del DPO y del Área de Seguridad antes de formalizar la contratación.

4.6.3. Sub-encargados

El Encargado no podrá subcontratar Tratamientos que involucren Datos Personales sin la autorización previa y por escrito de Integratel.

En caso de que dicha autorización sea otorgada, el Encargado deberá garantizar contractualmente que el Sub-encargado asuma obligaciones en materia de protección de Datos Personales equivalentes o, en todo caso, no menores a las establecidas en el DPA.

El Encargado mantendrá plena responsabilidad frente a Integratel por las actuaciones u omisiones del Sub-encargado, como si fueran propias.

4.6.4. Monitoreo y supervisión

La firma del DPA no exime de supervisión posterior. El Responsable Interno deberá:

- Supervisar el cumplimiento de las obligaciones contractuales.
- Reportar incidentes o incumplimientos detectados.
- Coordinar con el DPO y Seguridad cuando se identifiquen riesgos relevantes.

La supervisión podrá incluir revisiones documentales, validaciones técnicas o requerimientos de información cuando el riesgo lo amerite.

4.6.5. Supresión o devolución al término del contrato

Concluida la prestación contractual:

- El Encargado deberá suprimir o devolver los Datos Personales objeto de Tratamiento.
- No podrá conservar información salvo obligación legal debidamente acreditada.
- Deberá acreditar el cumplimiento de esta obligación cuando sea requerido.

La conservación indebida de Datos Personales constituye incumplimiento contractual.

4.6.6. Transferencias internacionales

Toda transferencia internacional de Datos Personales deberá:

- Ser evaluada previamente desde una perspectiva de riesgo.
- Garantizar un nivel adecuado de protección conforme a Legislación Vigente.
- Cuando el país de destino no cuente con un nivel adecuado de protección, incorporar garantías contractuales u otros mecanismos que aseguren un estándar equivalente de protección, tales como Acuerdos de Transferencia u otras cláusulas contractuales.
- Ser informada al DPO para su validación y registro.

No podrán realizarse transferencias internacionales sin análisis previo y documentación que sustente de la decisión adoptada.

4.7. Modelo de Gobernanza y responsabilidades

Las funciones descritas en el presente capítulo corresponden a los órganos y roles responsables de la dirección, supervisión y control del sistema de protección de Datos Personales de Integratel.

4.7.1. Gerencia General y Comité de Dirección

Son responsabilidades del Gerente General y del Comité de Dirección de Integratel impulsar el cumplimiento de la presente Normativa en todas las áreas.

4.7.2. Oficial de Datos Personales (DPO)

El DPO supervisa el cumplimiento de la presente Normativa. Sus funciones incluyen:

- Asesorar a las áreas en temas de protección de Datos Personales.
- Supervisar la implementación de la presente Normativa.
- Gestionar incidentes en coordinación con Seguridad y evaluar notificaciones.
- Mantener inventarios y documentación, en coordinación con TI y los Responsables Internos.
- Actuar como punto de contacto ante la Autoridad.
- Reportar periódicamente a Gerencia General.

El DPO no sustituye la responsabilidad de la gestión de los Tratamientos que realizan las áreas responsables descritas a lo largo de la presente Normativa.

4.7.3. Responsable Interno del Tratamiento

Es responsable de asegurar la implementación efectiva de las disposiciones establecidas en la presente Normativa respecto de los Tratamientos bajo su ámbito, en coordinación con el DPO y Seguridad. Le corresponde:

- Definir la finalidad específica del Tratamiento.
- Garantizar el cumplimiento del deber de información previo a la recolección de Datos Personales.
- Evaluar previamente los riesgos asociados al Tratamiento y coordinar, cuando corresponda, con el Área de Seguridad y el DPO.
- Asegurar que solo se traten los datos estrictamente necesarios conforme a la finalidad definida.
- Supervisar a los Encargados de Tratamiento y verificar el cumplimiento de las obligaciones contractuales.
- Implementar las medidas de seguridad definidas por el Área de Seguridad y verificar su aplicación en su ámbito.
- Garantizar la correcta conservación, bloqueo o eliminación de los datos conforme a la finalidad y a la normativa vigente.
- Informar al DPO sobre cambios relevantes vinculados al Tratamiento, incluyendo nuevas finalidades, incorporación de Proveedores, Flujo Transfronterizo o Incidentes de Seguridad.

El Responsable Interno mantiene responsabilidad operativa sobre los Tratamientos bajo su ámbito, sin perjuicio de la función de supervisión ejercida por el DPO.

4.7.4. Área de Seguridad

Las siguientes funciones describen las principales responsabilidades del Área de Seguridad en materia de protección de Datos Personales. La enumeración no es limitativa y podrá ampliarse en función de la naturaleza del Tratamiento, el nivel de riesgo identificado y las disposiciones internas aplicables:

- Determinar las medidas de seguridad proporcionales al nivel de riesgo identificado.

- Verificar y supervisar la implementación efectiva de las medidas de seguridad por parte de los Responsables Internos.
- Brindar soporte técnico a los Responsables Internos antes, durante y al finalizar un tratamiento de Datos Personales, en coordinación con el DPO.
- Evaluar riesgos técnicos asociados a nuevos Tratamientos, herramientas, integraciones y Activos Tecnológicos.
- Monitorear eventos de seguridad que puedan afectar la confidencialidad, integridad o disponibilidad de los Datos Personales.
- Gestionar vulnerabilidades y coordinar acciones correctivas.
- Administrar y actualizar el registro de Incidentes de Seguridad, en coordinación con el DPO.
- Coordinar con los Responsables Internos que correspondan y brindar contención inmediata ante Incidentes de Seguridad detectados.
- Realizar la evaluación y análisis forense de Incidentes de Seguridad.
- Mantener mecanismos de detección temprana de eventos anómalos.
- Participar en Evaluaciones de Impacto cuando el riesgo lo amerite.

El Área de Seguridad no sustituye la responsabilidad operativa del Responsable Interno del Tratamiento, pero actúa como órgano especializado de soporte y supervisión en materia de seguridad.

4.8. Responsabilidades operativas de las áreas

Las siguientes áreas de Integratel cumplen un rol relevante en la implementación de la presente Normativa. No obstante, la observancia de sus disposiciones es obligatoria para todas las áreas de la Compañía, conforme a sus funciones y responsabilidades:

4.8.1. Área de Tecnología de la Información (TI)

Serán responsabilidades de TI, como mínimo, las siguientes:

- Mantener actualizado el inventario de Activos.
- Administrar accesos y privilegios, bajo su gestión en coordinación con Seguridad.
- Implementar medidas de eliminación segura, cuando corresponda.
- Apoyar en la conservación de logs y trazabilidad.

4.8.2. Área Legal y Regulación

Serán responsabilidades de Legal y Regulación, como mínimo, las siguientes:

- Incorporar cláusulas contractuales necesarias.
- Asesorar en análisis legales y regulatorios en coordinación con el DPO.
- Gestionar procedimientos contenciosos ante la Autoridad.

4.8.3. Área de Personas

Serán responsabilidades de Personas, como mínimo, las siguientes:

- Incorporar obligaciones de confidencialidad y protección de Datos Personales en los contratos de trabajo, Reglamento Interno de Trabajo y otros documentos a su cargo.
- Gestionar capacitaciones obligatorias a los Trabajadores de Integratel en materia de protección de Datos Personales, en coordinación con el DPO.
- Aplicar régimen disciplinario cuando corresponda.

4.8.4. Auditoría Interna

Serán responsabilidades de Auditoría Interna, como mínimo, las siguientes:

- Verificar el cumplimiento documentado de la presente Normativa.
- Evaluar la eficacia de los controles.
- Formular recomendaciones de mejora.

4.9. Obligaciones individuales

4.9.1. Obligaciones de los Trabajadores

Todo trabajador que tenga acceso a Datos Personales en la Compañía, deberá:

- Utilizar los Datos Personales únicamente para fines autorizados.
- Acceder solo a la información necesaria para sus funciones.
- Mantener confidencialidad permanente.
- No extraer bases de Datos Personales sin autorización.
- No compartir credenciales.
- Reportar de manera inmediata cualquier incidente.

El uso indebido podría generar consecuencias disciplinarias y legales.

4.9.2. Obligaciones de los Proveedores

Los Proveedores en su condición de Encargados del Tratamiento deberán cumplir estrictamente lo establecido en el DPA y en la presente Normativa, aplicando medidas proporcionales al riesgo y reportando de manera inmediata cualquier incidente.

Los Proveedores deberán cumplir en todo momento con los niveles de calidad exigidos por Integratel. La Compañía se reserva el derecho de realizar, en cualquier momento y sin necesidad de comunicación previa, inspecciones, auditorías, revisiones, evaluaciones y visitas, ya sea directamente o a través de terceros designados, en cualquier instalación o sistema vinculado a la ejecución del Contrato, con la finalidad de verificar el cumplimiento de los niveles de servicio, las obligaciones contractuales asumidas y, cuando corresponda, la correcta implementación de las medidas de seguridad aplicables a los Datos Personales objeto del encargo.

La ejecución de dichas acciones no exime al Proveedor de su responsabilidad. El Proveedor se obliga a entregar a Integratel, o a quien ésta designe, toda la información y documentación que se le requiera.

4.10. Consecuencias del incumplimiento

4.10.1. Para Trabajadores

El incumplimiento de la presente Normativa constituye una falta grave que puede afectar directamente la continuidad operativa de Integratel. Podría generar:

- Medidas disciplinarias internas.
- Responsabilidad administrativa ante la Autoridad.
- Responsabilidad civil por daños y perjuicios.
- Responsabilidad penal conforme al Código Penal y a la Ley de Delitos Informáticos.

Se recuerda que conductas que impliquen uso indebido, uso no autorizado de archivos, extracción ilícita o tráfico ilegal de Datos Personales, pueden constituir delito y generar responsabilidad penal individual, incluyendo pena privativa de libertad.

4.10.2. Para Proveedores

El incumplimiento por parte de los Proveedores de las obligaciones establecidas en la presente Normativa y en el correspondiente DPA podrá generar las siguientes consecuencias, sin perjuicio de otras previstas en el contrato principal o en la Legislación Vigente:

- Aplicación de penalidades contractuales.
- Exigencia de medidas correctivas inmediatas.
- Suspensión temporal del servicio.
- Resolución del contrato por incumplimiento.
- Exigencia de indemnización por los daños y perjuicios ocasionados.
- Comunicación del incumplimiento a las autoridades competentes cuando corresponda.

Cuando el incumplimiento del Encargado genere responsabilidad administrativa frente a la Autoridad Nacional de Protección de Datos Personales, Integratel podrá ejercer las acciones legales correspondientes para repetir contra el Proveedor los costos, multas o sanciones que le sean atribuibles.

El Proveedor será responsable por las actuaciones de sus Sub-encargados y por cualquier Tratamiento realizado fuera del alcance autorizado.

Las conductas que impliquen uso indebido, revelación no autorizada, extracción ilícita o comercialización de Datos Personales podrán generar responsabilidad penal individual conforme al Código Penal y a la Ley de Delitos Informáticos.

5. Entrada en vigor

La presente Normativa entrará en vigor a partir de la fecha de su aprobación por el Directorio. El área de Regulación será responsable de su custodia, seguimiento y actualización, en coordinación con las áreas involucradas.

Asimismo, será objeto de revisión periódica, al menos una vez al año, a fin de evaluar su vigencia, eficacia y alineamiento con la normativa aplicable y los riesgos identificados. Podrá ser modificada cuando se produzcan cambios normativos, tecnológicos, organizacionales o cuando se identifiquen riesgos relevantes que así lo ameriten.

6. Anexos

La presente Normativa cuenta con ocho (08) anexos, los mismos que podrán actualizarse o incrementarse, de acuerdo con la Legislación Vigente y/o las necesidades de Integratel:

Anexo 1:	Política de Privacidad para Trabajadores de Integratel.
Anexo 2:	Cláusula de Protección de Datos Personales en Contratos de Trabajo.
Anexo 3:	Política de Privacidad de Clientes.
Anexo 4:	Cláusulas en contratos de abonados (Clientes): Tratamiento de Datos Personales (informativas) y Consentimiento Ofertas Comerciales.
Anexo 5:	Formato ARCO.
Anexo 6:	Política de Cookies.
Anexo 7:	Contrato de Encargo de Tratamiento de Datos Personales – DPA. Incluye Medidas de Seguridad y Plantilla de Notificación de Incidentes de Seguridad y Acuerdo de Transferencia (cláusulas contractuales tipo).
Anexo 8:	Declaración Jurada: Devolución/Supresión de la Información (datos personales).

ANEXO 1

POLÍTICA DE PRIVACIDAD PARA TRABAJADORES DE INTEGRATEL[8]

1. Responsable del Tratamiento

INTEGRATEL PERU S.A.A. (en adelante, "INTEGRATEL") identificada con RUC Nº 20100017491 y domiciliada en Jirón Domingo Martinez de Luján Nº 1130, Surquillo, Lima es la responsable del tratamiento de los Datos Personales de Trabajadores de INTEGRATEL. En consecuencia, ha registrado ante el Registro Nacional de Protección de Datos Personales, los bancos de Datos Personales denominados: "Trabajadores" con código RNPDP-PJP N°16216 y "Videovigilancia" con código: RNPDP-PJP N° 16218.

2. Finalidad

El presente documento (en adelante, la "Política de Privacidad") tiene como objetivo proporcionar a todas las personas naturales que mantienen una relación contractual de carácter laboral con INTEGRATEL (en adelante, el "Trabajador" o los "Trabajadores"), la información relativa al tratamiento de Datos Personales que realiza INTEGRATEL en el marco de la celebración y ejecución del contrato laboral.

INTEGRATEL podrá trasladar al Trabajador información adicional mediante cláusulas específicas o avisos de privacidad en documentos, formularios, notificaciones, sistemas y/o plataformas de INTEGRATEL.

3. Base Legal

INTEGRATEL realiza el tratamiento de los Datos Personales de los Trabajadores conforme a la Ley Nº 29733 – Ley de Protección de Datos Personales y su Reglamento aprobado mediante Decreto Supremo Nº 016-2024- JUS o las normas que las pudieran modificar o sustituir, así como las directivas o lineamientos que pueda emitir la Autoridad Nacional de Protección de Datos Personales.

4. Datos Personales Tratados

INTEGRATEL podrá tratar las siguientes categorías de Datos Personales de sus Trabajadores, según corresponda al vínculo laboral y las funciones desempeñadas:

a) Datos proporcionados directamente por el Trabajador

- Datos identificativos y de contacto.
- Información económica y bancaria para fines de pago.
- Información académica y experiencia profesional.
- Información necesaria para la gestión contractual y administrativa.
- Información de terceros cuando sea necesaria para beneficios o seguros.

b) Datos generados en el marco de la relación laboral

- Información relacionada con el vínculo laboral, tales como cargo, funciones, evaluaciones de desempeño, asistencia y cumplimiento de obligaciones laborales.
- Información relativa a salud ocupacional y prevención de riesgos laborales, conforme a la Legislación Vigente.
- Registros de control de acceso a instalaciones y sistemas de la Compañía.
- Información derivada del uso de redes, herramientas, sistemas, plataformas y dispositivos corporativos, conforme a las políticas internas y dentro de los límites legales.

[8] El presente documento cumple con la obligación de publicar "Políticas de Privacidad", dispuesta en el artículo 18° de la Ley Nº 29733 – Ley de Protección de Datos Personales y el artículo 7° de su Reglamento, aprobado mediante Decreto Supremo Nº 016-2024- JUS.

5. Finalidades del Tratamiento

Los Datos Personales de los Trabajadores serán tratados principalmente para la gestión del vínculo laboral y el cumplimiento de obligaciones legales y contractuales, incluyendo:

- Administración del contrato de trabajo.
- Gestión de remuneraciones y beneficios sociales.
- Cumplimiento de obligaciones tributarias, laborales y de seguridad social.
- Evaluaciones de desempeño y desarrollo profesional.
- Gestión de capacitaciones vinculadas al desempeño del cargo.
- Seguridad y control de acceso a instalaciones y sistemas.
- Gestión de directorios internos corporativos, incluyendo imagen cuando corresponda.

Adicionalmente, INTEGRATEL podrá tratar los Datos Personales para el ofrecimiento de beneficios corporativos no directamente vinculados a la ejecución del contrato de trabajo (por ejemplo, convenios con terceros), en cuyo caso se informará adecuadamente al Trabajador y, cuando corresponda, se recabará su consentimiento previo. En caso dichos beneficios impliquen la comunicación de Datos Personales a terceros, se adoptarán las medidas necesarias para garantizar el cumplimiento de la Legislación Vigente.

6. Transferencia de Datos

Para el cumplimiento de las finalidades antes descritas, LA EMPRESA podrá comunicar o encargar el tratamiento de los Datos Personales a las siguientes categorías de Terceros:

- Entidades públicas y autoridades competentes, cuando exista obligación legal.
- Entidades financieras para el pago de remuneraciones.
- Compañías aseguradoras y administradoras de fondos de pensiones.
- Proveedores de servicios de planillas, gestión de recursos humanos y soporte tecnológico.
- Proveedores de salud ocupacional y prevención de riesgos laborales.
- Dichos terceros actuarán conforme a la Legislación Vigente y, cuando corresponda, en calidad de encargados de tratamiento bajo contrato.

En caso LA EMPRESA ofrezca beneficios corporativos adicionales no vinculados directamente a la ejecución del contrato de trabajo (por ejemplo, convenios voluntarios con terceros), se informará previamente al (la) TRABAJADOR(A) sobre la identidad del tercero involucrado, la finalidad específica y los datos a compartir, y se recabará el consentimiento cuando corresponda.

Asimismo, INTEGRATEL le informa que sus Datos Personales realizarán flujo transfronterizo a los Estados Unidos de América como consecuencia del servicio contratado con Microsoft Corporation para la gestión del correo electrónico, almacenamiento en la nube, colaboración en línea.

7. Medidas de Seguridad

INTEGRATEL ha implementado medidas técnicas, organizativas y legales para garantizar la confidencialidad, integridad y disponibilidad de sus Datos Personales tratados.

8. Derechos del Titular del Dato

INTEGRATEL ha designado un Oficial de Datos Personales (DPO), quien es el encargado de velar por la protección de su derecho fundamental a la protección de Datos Personales al interior de la compañía. Para ejercer sus derechos de acceso, rectificación, cancelación y oposición (ARCO), deberá formular una solicitud escrita al siguiente correo electrónico:

protecciondedatos.pe@integratel.com.pe

9. Plazo de Conservación

Sus Datos Personales serán conservados por INTEGRATEL durante la vigencia de su vínculo laboral con ésta y una vez finalizada, se mantendrán bloqueados, únicamente por el plazo necesario para poder el cumplir con las obligaciones legales o el ejercicio de derechos en sede administrativa o judicial

10. Modificaciones

Esta Política de Privacidad podrá ser modificada y/o actualizada en cualquier momento por INTEGRATEL. Cualquier modificación y/o actualización le será comunicada oportunamente.

****

Declaro haber sido informado(a) de la presente Política de Privacidad para Trabajadores de INTEGRATEL.

Nombre:	
Apellidos	
DNI:	
Fecha:	
Firma:	

ANEXO 2

CLÁUSULA DE PROTECCIÓN DE DATOS PERSONALES
Contratos laborales

En cumplimiento de la Ley N° 29733 – Ley de Protección de Datos Personales, su Reglamento aprobado por Decreto Supremo N° 016-2024-JUS y demás Legislación Vigente, se informa a EL(LA) TRABAJADOR(A) que sus Datos Personales proporcionados durante el proceso de selección y contratación, así como aquéllos que se generen durante el desarrollo de su relación laboral, serán tratados por LA EMPRESA, para las siguientes finalidades principales:

i. Gestionar, ejecutar y administrar la relación laboral, incluyendo el cumplimiento de obligaciones legales, contractuales, tributarias y de seguridad social.

ii. Administrar remuneraciones, beneficios sociales, seguros y demás conceptos derivados del vínculo laboral.

iii. Evaluar el desempeño, cumplimiento de funciones y desarrollo profesional conforme al cargo asignado.
iv. Gestionar capacitaciones, formación y actividades vinculadas al desempeño profesional.

El tratamiento de Datos Personales para finalidades distintas a las necesarias para la ejecución del contrato de trabajo requerirá el consentimiento previo, libre, informado y expreso del (la) TRABAJADOR(A), cuando así lo exija la Legislación Vigente.

La información proporcionada por EL(LA) TRABAJADOR(A) debe ser exacta y veraz; siendo su responsabilidad comunicar cualquier actualización. Los Datos Personales serán tratados durante la vigencia de la relación laboral entre EL(LA) TRABAJADOR(A) y LA EMPRESA, y una vez finalizada, serán conservados bloqueados, únicamente por el plazo necesario para el cumplimiento de obligaciones legales o el ejercicio de derechos en sede administrativa o judicial.

EL(LA) TRABAJADOR(A) podrá ejercer sus derechos de acceso, rectificación, supresión y oposición dirigiéndose al área de Personas de LA EMPRESA o al correo electrónico: protecciondedatos.pe@integratel.com.pe, aportando copia de su documento de identidad o documentación equivalente, para acreditar su identidad.

Para mayor detalle sobre el tratamiento de los Datos Personales, lo invitamos a revisar la Política de Privacidad para Trabajadores de INTEGRATEL, que forma parte la Normativa de Protección de Datos Personales de INTEGRATEL, disponible en https://integratel.com.pe/politicas-relevantes-2 .

ANEXO 3

POLÍTICA DE PRIVACIDAD PARA CLIENTES

1.Responsable del tratamiento

INTEGRATEL PERÚ S.A.A. (en adelante, "INTEGRATEL"), con RUC N° 20100017491 y domicilio en Jirón Domingo Martínez Luján 1130, distrito de Surquillo – Lima, es responsable del tratamiento de los Datos Personales de sus Clientes.

Para efectos de la presente Política:

- **Cliente** es la persona natural que contrata uno o más servicios o adquiere productos de INTEGRATEL.

Los Datos Personales de Clientes son almacenados en el Banco de Datos Personales denominado "Clientes", de titularidad de INTEGRATEL, inscrito ante el Registro Nacional de Protección de Datos Personales con código RNPDP N° 13571.

Puede contactar al Oficial de Datos al correo: protecciondedatos.pe@integratel.com.pe .

La presente Política ha sido elaborada conforme a la Ley N° 29733 y su Reglamento aprobado por Decreto Supremo N° 016-2024-JUS.

2. Finalidades del tratamiento

2.1 Finalidades necesarias para la relación contractual

INTEGRATEL trata los Datos Personales para la preparación, celebración y ejecución de la relación contractual, incluyendo: identificación del Cliente, validación de identidad, evaluación crediticia, prestación de servicios contratados, facturación y cobranza, atención de consultas y reclamos, así como para el cumplimiento de obligaciones regulatorias y legales.

Para efectos de validación de identidad, INTEGRATEL podrá utilizar mecanismos de verificación biométrica administrados por RENIEC y/o MIGRACIONES, así como otros mecanismos legalmente habilitados.

Asimismo, podrá tratar información adicional estrictamente necesaria para prevenir fraude o suplantación de identidad, incluyendo la geolocalización del proceso de contratación cuando corresponda.

INTEGRATEL podrá utilizar herramientas tecnológicas basadas en inteligencia artificial para optimizar la atención de reclamos, reportes de averías y solicitudes de soporte, incluyendo el análisis automatizado de comunicaciones y registros asociados al servicio. Estas herramientas se emplearán exclusivamente para mejorar la calidad, eficiencia y tiempos de respuesta, bajo criterios de seguridad, confidencialidad y proporcionalidad, y conforme a la normativa vigente en materia de protección de datos personales.

La negativa a proporcionar los Datos Personales necesarios impedirá la contratación o prestación del servicio solicitado.

2.2 Finalidades adicionales

Con consentimiento previo, libre, expreso e informado, INTEGRATEL podrá: enviar comunicaciones comerciales, ofrecer promociones personalizadas, y realizar análisis de preferencias y consumo. Para ello podrá elaborar perfiles comerciales basados en información pertinente y proporcional.

El Cliente podrá oponerse en cualquier momento al tratamiento con fines comerciales.

3. Base legal del tratamiento

El tratamiento de Datos Personales de Clientes se sustenta en la ejecución de la relación contractual, el cumplimiento de obligaciones legales y el consentimiento del titular del Dato Personal cuando corresponda.

4. Conservación de los datos

Los Datos Personales de Clientes serán conservados durante el tiempo necesario para cumplir la finalidad que motivó su recopilación y, posteriormente, durante los plazos exigidos por obligaciones legales o regulatorias aplicables.

5. Destinatarios de los datos

INTEGRATEL podrá compartir Datos Personales de sus Clientes, de ser aplicable, con: proveedores que actúan como encargados de tratamiento, entidades públicas cuando exista obligación legal, y sistemas de información crediticia en caso de incumplimiento de obligaciones dinerarias.

Todos los proveedores están sujetos a obligaciones contractuales de confidencialidad y seguridad. Ver lista aquí.

6. Transferencias internacionales

En algunos casos, INTEGRATEL podrá transferir los Datos Personales de sus Clientes a proveedores fuera del Perú cuando ello sea necesario para la prestación de los servicios contratados o para cumplir las finalidades informadas en esta Política. Estas transferencias se realizarán únicamente cuando:

- El país de destino cuente con un nivel adecuado de protección de Datos Personales; o
- Se hayan establecido garantías contractuales que aseguren que sus Datos Personales recibirán un nivel de protección equivalente al exigido por la Legislación Vigente.

En todos los casos, INTEGRATEL adoptará las medidas necesarias para proteger su información y garantizar el respeto de sus derechos.

7. Medidas de Seguridad

INTEGRATEL implementa medidas técnicas y organizativas apropiadas para proteger los Datos Personales de sus Clientes contra pérdida, alteración, acceso no autorizado o uso indebido.

8. Derechos del Cliente

El Cliente o Usuario en su condición de titular del dato puede ejercer los siguientes derechos ARCO: Acceso, Rectificación, Cancelación, Oposición, e Información.

Para ello podrá descargar su solicitud ARCO **aquí** , completarla, firmarla y remitirla adjuntando copia de su documento de identidad al correo: protecciondedatos.pe@integratel.com.pe.

Asimismo, podrá ejercer sus derechos en nuestros Centros de Atención Movistar a nivel nacional.

Plazos de atención: Acceso: 20 días hábiles. Rectificación, cancelación y oposición: 10 días hábiles. Información: 8 días hábiles.

Además de los anteriores derechos, el Cliente tendrá derecho a retirar el consentimiento otorgado en cualquier momento mediante el procedimiento más arriba descrito, sin que dicha retirada de consentimiento afecte a la licitud del tratamiento anterior a la retirada del mismo. De considerar que no ha sido atendido en el ejercicio de sus derechos puede presentar una reclamación ante la Autoridad Nacional de Protección de Datos Personales vía correo electrónico: protegetusdatos@minjus.gob.pe

9. Uso de cookies

INTEGRATEL utiliza cookies para mejorar la experiencia de navegación y ofrecer contenidos personalizados. El Cliente que, en calidad de usuario, accede a los sitios web de INTEGRATEL puede aceptar o rechazar su uso conforme a la Política de Cookies disponible.

11. Modificaciones

INTEGRATEL podrá actualizar la presente Política para reflejar cambios normativos o operativos. La versión vigente estará disponible en su sitio web: https://centrodetransparencia.movistar.com.pe/politica-de-cookies

ANEXO 4

CLÁUSULAS CONTRATO DE ABONADOS

TRATAMIENTO DE DATOS PERSONALES

Te informamos que la entrega de tus Datos Personales es necesaria para brindarte el servicio contratado. INTEGRATEL y sus encargados procesarán tus datos bajo estrictas medidas de seguridad para velar por su confidencialidad conforme a nuestra Política de Privacidad disponible en www.movistar.com.pe/privacidad. Podrás ejercer tus derechos de acceso, rectificación, cancelación, y oposición en nuestros centros de atención o enviando un correo a protecciondedatos.pe@integratel.com.pe, adjuntando copia de tu documento de identidad.

CONSENTIMIENTO OFERTAS COMERCIALES

En función a tus gustos y/o comportamiento recopilado a través de nuestros sitios web, te enviaremos ofertas comerciales personalizadas, a través de medios escritos, verbales o electrónicos/informáticos. Para ello, contamos con tu autorización para elaborar tu perfil de manera automatizada usando tus datos demográficos, económicos, comerciales, de tráfico y de localización.

☐ Sí, acepto.

☐ No acepto.

ANEXO 5

FORMATO DE SOLICITUDES ARCO

Protección de Datos Personales
Ley N° 29733

Fecha de presentación:		
N° Documento de Identidad del Titular:		
Datos del Titular (*):		
Nombres		
Apellidos		
Teléfono de contacto:		
Correo electrónico:		
Indicar si es cliente de Movistar:		
Marcar con un X	SI	NO

(*) Deberá adjuntar a la presente solicitud, copia simple de los documentos que acrediten la identidad del titular (Documento Nacional de Identidad o documento equivalente).

Tipo de Solicitud. Seleccione el tipo de solicitud a realizar:

☐	Acceso	(acceder a sus Datos Personales que obren en las bases de datos de la empresa)
☐	Rectificación	(rectificar o actualizar Datos Personales en el banco de datos de la empresa)
☐	Cancelación	(supresión o cancelación de Datos Personales)
☐	Oposición	(oponerse al tratamiento de los Datos Personales)

Descripción de la solicitud:

_____

_____

_____

Firma del solicitante _____

Nombres y apellidos: _____

Documento de Identidad: _____

ANEXO 6

POLÍTICA DE COOKIES

La presente Política de Cookies tiene como finalidad facilitar a todos los usuarios y visitantes de las URLs https://www.movistar.com.pe y https://tiendaonline.movistar.com.pe (en adelante, la "Web") información clara y completa sobre la utilización y funcionamiento de las Cookies alojadas en ellas.

Las Cookies pueden ser definidas como archivos temporales que se almacenan en los equipos de los usuarios a fin de recopilar cierta información sobre su experiencia de navegación y sobre sus preferencias.

La utilización de las Cookies persigue, por un lado, implementar en la Web las mejoras técnicas que permitan optimizar su funcionamiento, y, por otro, conocer las preferencias de los usuarios con el objetivo de adecuar nuestro contenido a dichas preferencias.

Las Cookies no suponen ningún daño para los equipos de los usuarios ni perjudican en absoluto su funcionamiento. Además, las Cookies pueden ser habilitadas o deshabilitadas en cualquier momento por los usuarios accediendo de forma sencilla al apartado de configuración de privacidad que facilitan los navegadores más convencionales.

Tipología de las Cookies alojadas en la Web

a. Cookies Propias

b. Cookies de Terceros. Cookies de Google Analytics y otras herramientas publicitarias.

Consentimiento de los usuarios para el funcionamiento de las Cookies

El usuario y el visitante de la Web conoce y acepta que INTEGRATEL podrá utilizar un sistema de seguimiento mediante utilización de Cookies.

Adicionalmente, se ponen a disposición de los usuarios en este apartado todas las indicaciones necesarias para que puedan configurar el funcionamiento y/o eliminar las Cookies ya instaladas, en los navegadores más habituales:

- Internet Explorer: https://windows.microsoft.com/es-es/windows-vista/block-or-allow-cookies
- Safari: https://www.apple.com/es/privacy/use-of-cookies
- Opera: https://help.opera.com/Windows/11.50/es-ES/cookies.html
- Chrome: https://support.google.com/chrome/bin/answer.py?hl=es&answer=95647

Se advierte a los usuarios de que, en caso de que desactiven en su navegador el funcionamiento de las Cookies, es posible que su experiencia de navegación en la Web no sea óptima.

ANEXO 7

CONTRATO DE ENCARGO DE TRATAMIENTO DE DATOS PERSONALES CON ACUERDO DE FLUJO TRANSFRONTERIZO (en adelante el "Contrato de Encargo" o "DPA")

INTEGRATEL PERÚ S.A.A. identificada con RUC N° 20100017491, en su calidad de **Responsable del Tratamiento** (el "**Responsable**"); y _____ identificada con _____ N° _____ en su calidad de **Encargado del Tratamiento**[9] (el "**Encargado**"). El **Responsable** y el **Encargado,** podrán ser denominados individualmente como la "**Parte**" y conjuntamente las "**Partes**".

La naturaleza y tipología de los **Datos Personales**, así como la finalidad del **Tratamiento de Datos Personales** materia del presente encargo, se encuentran detalladas en el **Apéndice 3** del presente **DPA.**

1. Objeto

El presente **DPA** tiene por objeto regular el **Tratamiento de Datos Personales** que el **Encargado** realice por cuenta u orden del **Responsable**, en el marco de la prestación de los servicios contratados conforme al **Contrato Principal u Orden de Compra**, del cual este **DPA** forma parte integrante.

El **Encargado** se obliga a cumplir con la Ley N.° 29733, su Reglamento - D.S. N.° 016-2024-JUS, y toda norma que las modifique, sustituya y complemente[10] (la "**Legislación Vigente**"). La naturaleza de los **Datos Personales**, las finalidades y las operaciones de **Tratamiento** se detallan en el **Apéndice 3.**

2. Definiciones

- **"Datos Personales":** Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.
- **"Datos sensibles":** Información relativa a datos genéticos o biométricos de la persona natural, datos neuronales, datos morales, hechos o circunstancias de su vida sexual, afectiva o familiar, los hábitos personales de su esfera más íntima, la información relativa a la afiliación sindical, salud física o mental u otras que afecten su intimidad. Datos referidos al origen racial y étnico; ingresos económicos; opiniones políticas, religiosas, filosóficas o morales.
- **"Emisor de Datos Personales"**: Es el responsable del **Tratamiento de Datos Personales**, situado dentro del territorio nacional y que realiza una **Transferencia internacional.**

[9] El Encargado de Tratamiento de Datos Personales actúa con la condición de proveedor del Responsable (Integratel).
[10] Se incluye la Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país – Ley N° 31814 y su Reglamento aprobado mediante Decreto Supremo N° 115-2025-PCM, de aplicar.

- **"Encargado del Tratamiento"**: Persona natural o jurídica, o entidad pública que trata los **Datos Personales** por cuenta u orden del **Responsable**.
- **"Incidente(s) de Seguridad":** 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.
- **"Oficial de Datos Personales"** (en adelante**, DPO**): Es la persona designada por el **Responsable del Tratamiento** o **Encargado del Tratamiento** para la verificación, asesoramiento e implementación del cumplimiento de la **Legislación Vigente.**
- **"Receptor de Datos Personales":** Es toda persona natural o jurídica de derecho privado, incluyendo las sucursales, filiales, vinculadas o similares o entidades públicas, que recibe los **Datos Personales** en caso de **Transferencia internacional.**
- **"Responsable del Tratamiento"**: Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y medios de los **Tratamientos de Datos Personales**.
- **"Sub-encargado del Tratamiento"** (en adelante, **el "Sub-encargado"**): Persona natural o jurídica, o entidad pública, a quien el **Encargado** subcontrata todo o parte del **Tratamiento de Datos Personales** que corresponda ejecutar al **Encargado** por cuenta u orden, y con la autorización previa del **Responsable.**
- **"Titular de Datos Personales"**: Persona natural a quien corresponden los **Datos Personales** materia de tratamiento. Las personas jurídicas no son sujeto de derechos al amparo de la **Legislación Vigente.**
- **"Transferencia internacional" o "Flujo Tranfronterizo"**: La transferencia de **Datos Personales** a un destinatario situado en un país distinto al país de origen de dichos datos por ejemplo, la transferencia de **Datos Personales** realizada fuera del territorio del **Responsable**.
- **"Tratamiento(s) de Datos Personales" o "Tratamiento(s)"**: 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 los **Datos Personales**.

3. Duración

Este **DPA** se mantendrá vigente hasta la finalización del **Contrato Principal u Orden de Compra**. De ampliarse la vigencia del **Contrato Principal,** y en tanto no se modifiquen las finalidades iniciales, el presente **DPA** se mantendrá vigente, sin necesidad de suscribir uno nuevo.

Lo anterior se entiende **sin perjuicio de las obligaciones que, por su naturaleza, deban subsistir con posterioridad** a la terminación del **Contrato Principal o del presente DPA.**

4. Compromisos del Encargado

El **Encargado** se obliga a tratar los **Datos Personales** únicamente por cuenta u orden del **Responsable**, conforme a las instrucciones documentadas previstas en el presente **DPA** y en el **Apéndice 3**, aplicando en todo momento las medidas de seguridad descritas en el **Apéndice 1**, y en estricto cumplimiento de la **Legislación Vigente**. En particular, y sin que la siguiente enumeración tenga carácter limitativo, el **Encargado** se compromete a:

4.1 Limitar el **Tratamiento de Datos Personales** a las finalidades expresamente autorizadas por el **Responsable**, quedando prohibido cualquier uso distinto o para fines propios. Todos los **Datos Personales**, así como los resultados derivados de su tratamiento —incluyendo elaboraciones, evaluaciones, segmentaciones, anonimización u otros procesos— serán de titularidad exclusiva del **Responsable**, en el marco de los servicios contratados.

4.2 Proporcionar al **Responsable**, cuando este lo solicite, información suficiente, veraz y actualizada sobre los **Tratamiento de Datos Personales** realizados por su cuenta, con el fin de permitir el cumplimiento de sus obligaciones legales, incluyendo la gestión de registros de tratamientos y/o bancos de **Datos Personales.** Dicha información comprenderá, como mínimo, datos de contacto y del **DPO** (de corresponder), descripción de los tratamientos efectuados, transferencias internacionales aplicables y una descripción general de las medidas de seguridad implementadas. El **Encargado** garantiza la exactitud y actualización de dicha información.

4.3 Asistir al **Responsable** en el cumplimiento de sus obligaciones en materia de protección de **Datos Personales**, incluyendo la atención de derechos de los titulares y la gestión de incidentes de seguridad, conforme a la **Legislación Vigente**. En caso el **Encargado** reciba directamente solicitudes de ejercicio de derechos, deberá comunicarlas al **Responsable** dentro del día hábil siguiente a su recepción, adjuntando la información relevante.

4.4 Suprimir o devolver al **Responsable** todos los **Datos Personales** tratados en el marco del presente **DPA** una vez finalizada la prestación de los servicios, a elección del **Responsable,** dentro de un plazo máximo de cinco (5) días calendario, así como los soportes que los contengan, cuando corresponda.

A solicitud del **Responsable**, el **Encargado** deberá acreditar el cumplimiento de esta obligación mediante certificación emitida por su **DPO,** representante autorizado o tercero independiente.

4.5 Garantizar que su personal autorizado cuente con la formación, sensibilización y compromisos de confidencialidad necesarios en materia de protección de Datos Personales, incluyendo el conocimiento y aplicación de las medidas de seguridad y de los procedimientos de gestión de incidentes previstos

en el presente **DPA**. Las obligaciones de confidencialidad subsistirán aun después de la finalización del **DPA.**

5. Medidas de Seguridad técnicas, organizativas y legales

5.1. El **Encargado** deberá implementar y mantener durante la vigencia del presente **DPA** las medidas técnicas, organizativas y legales apropiadas para garantizar un nivel de seguridad aceptable y equiparable al realizado por el **Responsable**, respecto del **Tratamiento de los Datos Personales** que realice por su cuenta u orden.

5.2. Las medidas de seguridad deberán determinarse considerando, entre otros factores, la naturaleza de los **Datos Personales** tratados, las finalidades del tratamiento, el volumen, el contexto operativo, los riesgos previsibles y las consecuencias potenciales para los **Titulares de los Datos Personales**.

5.3. Al valorar el nivel de seguridad adecuado, el **Encargado** se compromete a tener en cuenta, los riesgos presentados en el **Tratamiento**, en particular destrucción, pérdida y modificación accidentales o ilícitas, y la divulgación o al acceso no autorizados de **Datos Personales** bajo **Tratamiento.**

5.4. El **Encargado** se compromete a implementar las medidas de seguridad indicadas en el **Apéndice 1** del presente **DPA** que correspondan y a cumplir, particularmente, con aquellas establecidas en la **Legislación Vigente.**

5.5. El **Encargado** se obliga a monitorear adecuadamente el cumplimiento de las medidas técnicas, organizativas y legales implementadas, además de proporcionar las respectivas evidencias bajo petición del **Responsable**.

6. Subcontratación:

6.1. El **Responsable** autoriza al **Encargado** a subcontratar todo o parte de **los Tratamientos de Datos Personales** en el marco del presente **DPA**, a la lista de **Sub-encargados** contenida en el **Apéndice 3**. En caso se realice algún cambio en la lista de **Sub-encargados**, el **Encargado** deberá: (i) notificar por escrito al **Responsable** previamente detallando la incorporación o sustitución de aquel **Sub-Encargado**; y, (ii) otorgar al **Responsable** la oportunidad de oponerse a dichos cambios dentro de los diez (10) días calendario siguientes a su notificación.

6.2. El **Encargado** se obliga a suscribir con cada **Sub-encargado** un **DPA** mediante el cual el **Sub-encargado** se obligará a cumplir con las obligaciones del presente **DPA.** Asimismo, tanto el **Encargado** como el **Sub-Encargado** se obligan a seguir las instrucciones del **Responsable** en relación con el **Tratamiento de Datos Personales.**

6.3. En todo caso, el **Sub-encargado** asumirá las mismas obligaciones de protección de Datos Personales que las impuestas al **Encargado** en el presente **DPA.** Ante ello, el **Encargado** y el **Sub-encargado** responderán solidariamente frente al **Responsable** respecto de las acciones u omisiones del **Sub-encargado** que infrinjan lo pactado en el presente **DPA.**

7. Transferencias Internacionales

7.1 Las **Transferencias Internacionales** se darán en el marco de lo dispuesto por **la Legislación Vigente**, en particular, la determinación del nivel de protección adecuado de un país y las garantías del **Flujo Transfronterizo.**

7.2 En el caso de que el **Tratamiento de Datos Personales** materia del presente **DPA** se realice en un país que no cumpla con el requisito anterior, se hará uso de Cláusulas Contractuales Tipo u otros instrumentos jurídicos, en los que se establezcan cuando menos las mismas obligaciones a las que se encuentra sujeto el **Emisor**, así como las condiciones en las que el **Titular de Datos Personales** consintió el **Tratamiento de Datos Personales.**

7.3 Para la aplicación de lo señalado en la presente sección, se determinará quién actúa en calidad de **Emisor** (**Responsable, Encargado o Sub-encargado**) y quién en calidad de **Receptor**. El **Responsable** podrá decidir si firma directamente con el **Sub-encargado** o, por el contrario, requerirá que el **Encargado** firme dichas cláusulas con el **Sub-encargado** en nombre del **Responsable.**

8. Incidentes de Seguridad de Datos Personales

8.1 El **Encargado** notificará al **Responsable** de forma inmediata y sin dilación indebida cualquier **Incidente de Seguridad de Datos Personales**, real o presunto, del que tome conocimiento en el marco del presente **DPA**, utilizando los canales de contacto establecidos en el **Apéndice 3**.

8.2 Asimismo, el **Encargado** mantendrá un proceso documentado de gestión de incidentes, que abarque, como mínimo, su identificación, análisis, contención, mitigación, resolución, recuperación y cierre, y cooperará activamente con el **Responsable** en la investigación y gestión del incidente, poniendo a su disposición toda la información, registros, evidencias y personal que resulten necesarios.

8.3 Desde que tenga conocimiento del incidente, el **Encargado** adoptará, en coordinación con el **Responsable**, las medidas necesarias para mitigar sus efectos y ejecutará con la máxima diligencia las instrucciones que este le imparta en relación con dicho incidente, asegurando la disponibilidad de un contacto de seguridad para la atención continua del mismo.

9. Supervisión y Auditoría

9.1. El **Encargado** se obliga a cumplir con los niveles de calidad exigidos por el **Responsable** y con las obligaciones asumidas en el presente **DPA.** El **Responsable** queda autorizado para, en cualquier momento y sin necesidad de comunicación previa, realizar inspecciones, auditorías, revisiones, evaluaciones y visitas, directamente o a través de terceros, en cualquier instalación donde se ejecute el presente **DPA**, a fin de verificar el cumplimiento de los niveles exigidos y de las demás obligaciones del Encargado en el marco de la ejecución del presente **DPA**, incluso una vez finalizada la prestación de servicios establecida en el **DPA**.

9.2. La ejecución de dichas acciones no exime al **Encargado** de su responsabilidad. El **Encargado** se obliga a entregar al **Responsable**, o a quien ésta designe, toda la información y documentación que se le requiera. El **Encargado** permitirá la realización de auditorías de sus sistemas de información, incluidas inspecciones, por parte del **Responsable** o de otro auditor autorizado por el **Responsable** quien tendrá derecho de realizar cuantas auditorías y/o inspecciones estime convenientes al **Encargado**, para verificar el cumplimiento del presente **DPA.**

9.3. El **Encargado** pondrá a disposición del **Responsable**, en un plazo no mayor de treinta (30) días calendario desde la solicitud, toda la información necesaria para demostrar el cumplimiento de las obligaciones del presente **DPA**. El **Encargado** facilitará al **Responsable**, un ejemplar del **DPA** suscrito con el **Sub-encargado,** a fin de acreditar el cumplimiento. Lo anterior, sin perjuicio de las obligaciones de confidencialidad que pudieran existir entre ambos.

10. Responsabilidad

10.1 Las **Partes** responderán de las infracciones cometidas por cada una de ellas. No obstante, se obligan a mantenerse indemnes por aquellos daños y/o perjuicios que sufran como consecuencia de un incumplimiento por la otra parte de sus obligaciones como **Encargado, Sub-encargado o Responsable** en el marco del presente **DPA**, según el caso. A tal efecto, la parte incumplidora acepta indemnizar a la otra en la cantidad en que sea condenada en concepto de sanción, multa, principal e intereses, así como cualquier otro daño o perjuicio que se ocasione como consecuencia del mismo, incluidos los honorarios sustentados de abogado y procurador.

10.2 Sin perjuicio de lo anterior, el **Responsable** podrá repercutir directamente contra el **Encargado** o **Sub-encargado** cualquier sanción económica que pueda imponerle la autoridad competente como consecuencia de dicho incumplimiento.

10.3 El incumplimiento por parte del **Encargado** de cualquiera de las obligaciones establecidas en el presente **DPA** constituirá un incumplimiento contractual, sin perjuicio de las responsabilidades

administrativas, civiles o penales que pudieran corresponder conforme a la **Legislación Vigente**. Dicho incumplimiento será sancionado conforme a las penalidades y demás consecuencias previstas en el **Contrato Principal u Orden de Compra**, las cuales resultan plenamente aplicables al presente **DPA,** sin necesidad de requerimiento adicional.

11. Ley aplicable y jurisdicción

Cualquier cuestión relativa a la existencia, validez, incumplimiento o terminación de este **DPA**, y cualquier otra disputa que surja de este **DPA** o se relacione, se someterán a la jurisdicción exclusiva de los Tribunales del **Perú**, bajo la **Legislación Vigente.**

12. Apéndices:

Los Apéndices listados a continuación forman parte del presente **DPA**:

- Apéndice 1: Descripción de las **Medidas de Seguridad.**
- Apéndice 2: Plantilla de notificación ante **Incidentes de Seguridad de Datos Personales.**
- Apéndice 3: Cuestiones generales sobre el **Tratamiento de Datos Personales.**
- Apéndice 4: Acuerdo Modelo **de Transferencia Internacional de Datos Personales,** de aplicar.

Firma del Responsable

Nombre:	
Cargo:	

Firma del Encargado

Nombre:	
Cargo:	

APÉNDICE 1

MEDIDAS DE SEGURIDAD

Las medidas descritas en el presente Apéndice constituyen referencias mínimas orientativas y no tienen carácter taxativo, sin perjuicio de que el **Responsable** pueda exigir medidas adicionales o específicas en el **Contrato Principal u Orden de Compra**, o mediante instrucciones documentadas, en función del riesgo del **Tratamiento.**

1. Gestión de riesgos

El **Encargado** deberá:

- Contar con una metodología de análisis de riesgos basada en un marco estándar reconocido,
- Evaluar periódicamente los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y resiliencia de los **Datos Personales.**
- Monitoreo continuo de los planes de acción, analizando la eficacia de controles.
- Revisar la adecuación de sus medidas de seguridad ante cambios relevantes en los **Tratamientos,** tecnologías o amenazas.

2. Dominios de medidas de seguridad

En función del riesgo del **Tratamiento,** el **Encargado** deberá implementar medidas adecuadas dentro de los siguientes dominios, de manera proporcional y coherente con su modelo operativo:

(i) Protección del dato
Medidas de seudonimización, anonimización y cifrado de los **Datos Personales**, tanto en reposo como en tránsito, cuando resulte apropiado.

(ii) Confidencialidad, integridad y disponibilidad
Controles que permitan garantizar la protección continua de los sistemas, así como su resiliencia operativa.

(iii) Continuidad y recuperación
Medidas para restaurar la disponibilidad y el acceso a los **Datos Personales** de forma oportuna ante incidentes físicos o técnicos, incluyendo copias de seguridad.

(iv) Control de accesos e identidades
Mecanismos para la identificación, autenticación y autorización de usuarios, aplicando principios de mínimo privilegio, segregación de funciones y revocación oportuna de accesos.

(v) Seguridad de infraestructura y redes
Medidas para proteger los entornos tecnológicos, redes, dispositivos y comunicaciones, incluyendo segmentación, monitoreo y protección perimetral.

(vi) Seguridad física
Controles de acceso y protección de instalaciones, centros de procesamiento y soportes que contengan **Datos Personales.**

(vii) Desarrollo y cambios seguros
Medidas que aseguren la seguridad a lo largo del ciclo de vida del desarrollo, pruebas, despliegues y gestión de cambios, evitando el uso de datos reales en entornos no productivos cuando no corresponda.

(viii) Gestión de incidentes de seguridad
Procedimientos documentados para la detección, gestión, mitigación y reporte de Incidentes de Seguridad de **Datos Personales.**

(ix) Gobernanza y gestión de la seguridad
Políticas, roles, responsabilidades y estructuras internas que permitan una gestión efectiva de la seguridad de la información y protección de **Datos Personales.**

(x) Transferencias y comunicaciones
Medidas que aseguren la protección de los **Datos Personales** durante su transmisión, interconexión o transferencia, nacional o internacional.

(xi) Formación y concientización
Acciones de capacitación y sensibilización periódicas dirigidas al personal autorizado que trate **Datos Personales.**

(xii) Retención, portabilidad y supresión
Medidas que permitan gestionar adecuadamente los plazos de conservación, la portabilidad, la supresión y el borrado seguro de los **Datos Personales** conforme a las instrucciones del **Responsable**.

APÉNDICE 2

PLANTILLA DE NOTIFICACIÓN ANTE INCIDENTES DE SEGURIDAD DE DATOS PERSONALES

1	**Identificación del Encargado.**	**Completar por el Encargado** (*cuando corresponda)*
a.	Nombre del **Encargado** y/o el **Sub-encargado**, que detectó indicios u ocurrencia de un **Incidente de Seguridad** de los **Datos Personales** bajo cuenta u orden del **Responsable**.	
b.	Nombre y datos del **DPO** o de otro punto de contacto del **Encargado** autorizado, quien pueda proporcionar más información al **Responsable**.	
2	**Información inicial sobre un Incidente de Seguridad de Datos Personales**.	
a.	Fecha y hora del incidente **de Seguridad.**	
b.	Fecha y hora de la detección del **Incidente de Seguridad.**	
c.	Circunstancias en que se haya producido el **Incidente de Seguridad** (ej: pérdida, robo, etc.).	
d.	Tipos de los **Datos Personales** en cuestión, precisando si se trata de **Datos Sensibles**.	
e.	Medidas técnicas y organizativas que ha aplicado (o aplicará) el **Encargado** o **Sub-encargado**, según corresponda, a los **Datos Personales** en cuestión para mitigar los posibles efectos negativos.	
f.	Indicación de si se trata de una primera o segunda notificación del **Incidente de Seguridad**.	
3	**Información suplementaria del Incidente de Seguridad:**	
a.	Resumen y estado actual del **Incidente de Seguridad**.que ha causado o podría haber generado la vulneración de Datos Personales (con indicación de la ubicación física de la violación y del soporte de almacenamiento).	
b.	Número exacto o aproximado de **Titulares de Datos Personales** afectados.	
c.	Posibles consecuencias y efectos negativos en los titulares de Datos Personales.	
d.	Medidas de contención que ha adoptado el **Encargado** para mitigar el **Incidente de Seguridad** y sus posibles efectos negativos.	
e.	Si no es posible facilitar alguno de los campos de información antes descritos, se deberá identificar y remitir la información en la medida de lo posible y de manera gradual sin dilación indebida.	

APÉNDICE 3

CUESTIONES GENERALES SOBRE EL TRATAMIENTO

3.1. Completar por INTEGRATEL, como Responsable del Tratamiento de Datos Personales:

3.1.1 Naturaleza, Objeto y Finalidad del tratamiento *¿por qué y para qué el Proveedor tratará los Datos Personales?. Describir.*	
3.1.2. Detalles de contacto del responsable interno del Tratamiento materia de encargo.	Nombre: Correo: Teléfono: Área:
3.1.3 Detalles de contacto del DPO u Oficial de Datos Personales del Responsable	Nombre: Ana Claudia Quintanilla Correo:ana.quintanilla@integratel.com.pe Teléfono: 996317479
3.1.4 Dirección de correo del Responsable para la notificación de incidentes de protección de datos	gestionincidencias.pe@integratel.com.pe
3.1.5. Territorio:	**Perú**
3.1.6. Especificar las categorías de Datos Personales a tratar. *Seleccionar la categoría que corresponda.*	☐ Datos de carácter identificativo: nombres y apellidos, dirección, teléfono, correo electrónico, IMEI, IMSI, otros. ☐ Datos de características personales: profesión, género, nacionalidad, estado civil. ☐ Datos de carácter social: localización, tráfico, hábitos y preferencias. ☐ Datos económicos y financieros: transacciones, posiciones, ingresos, cuentas, facturas. ☐ Datos sensibles: de salud, ingresos económicos, biométricos, orientación sexual, etc. Especificar:
3.1.7. Categoría de titulares de datos *Seleccionar a quiénes pertenecen los Datos Personales a tratar*	☐ Trabajadores, postulantes ☐ Clientes, Prospectos ☐ Otros: especificar.
3.1.8. Duración del Tratamiento	Corresponde a la del **Contrato Principal u Orden de Compra** correspondiente; o si la duración del tratamiento difiere, la duración será la establecida específicamente por las **Partes**.

3.2. A completar por el PROVEEDOR en su condición de Encargado del Tratamiento:

3.2.1. Detalles de contacto del proveedor.	*Denominación social:* *Nombre del representante:* *Correo electrónico.*
3.2.2. Detalles de contacto del Oficial de Datos Personales o DPO del proveedor	*Nombre del DPO u Oficial de Datos Personales:* *Correo electrónico:*
3.2.3. Dirección del tratamiento por parte del proveedor	*Dirección física:*
3.2.4. Indicar las ubicaciones dónde el proveedor aloja los datos *(Seleccionar el que corresponda)*	☐ En el Perú. ☐ Fuera del Perú. Especificar ubicación:
3.2.5. Indicar desde donde el proveedor accede a los datos para dar soporte o prestar el servicio contratado *(Seleccionar el que corresponda)*	☐ En el Perú. ☐ Fuera del Perú. Especificar ubicación:
3.2.6. En base a lo consignado en el 3.2.4 y 3.2.5 confirmar lo siguiente: *(Seleccionar el que corresponda)*	En caso en los Apéndices 3.2.4 y/o 3.2.5 se consigne **"Fuera del Perú"**, y el país o páises consignados **no cuenten con un nivel de protección adecuado**[11], el **Encargado** deberá obligatoriamente: ☐ Suscribir el **Acuerdo Modelo de Transferencia Internacional de Datos Personales**, el cual forma parte integrante del presente DPA como **Apéndice 4**, como condición previa al inicio del flujo transfronterizo. La suscripción del **Apéndice 4** constituye un requisito indispensable para la validez del tratamiento fuera del Perú.

3.3. Subcontratistas. A continuación, detallar los **Sub-contratistas** del **Encargado del Tratamiento** para la prestación de los Servicios objeto del **Contrato Principal** u **Orden de Compra**.

[11] Ver lista de países con nivel de protección adecuado aquí: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

*(Nota: Los subcontratistas no declarados en el presente **DPA**, se tendrán como no autorizados por el **Responsable,** y configurará un incumplimiento contractual. El **Encargado** deberá previamente informar al **Responsable** cualquier modificación sobre este numeral y solicitar su autorización expresa).*

Nombre del Sub-contratista	**País/es desde los que se almacenan o acceden a Datos Personales**	**Finalidad de las Subcontrataciones**	**Datos de contacto del DPO y/o Área de Seguridad**	**En caso de una transferencia internacional de datos, garantía que aplica: Cláusulas Tipo, país adecuado, otra.**

3.4. Sistema basado en IA

Son Sistemas basados en IA aquellos basados en una máquina que, para objetivos de forma explícita o implícita, infiere a partir de la entrada que recibe, cómo generar salidas o tales como predicciones, contenido, recomendaciones o toma de decisiones que pueden influir en la o los entornos físicos o digitales.

		Marcar con "X" según corresponda
¿El Encargado o Sub-encargado declara haber evaluado y adecuado el uso de herramientas de inteligencia artificial, a lo dispuesto en la Ley N.° 31814, Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país, y su Reglamento aprobado mediante Decreto Supremo N.° 115-2025-PCM?	**SI**	
	No	

		Marcar con "X" según corresponda
¿El Encargado o Sub-encargado usa o usará Sistemas basados en IA en el Tratamiento de Datos Personales materia del presente DPA?	**SI**	
	No	

En caso el Encargado marque SI, detallar a continuación dichos Sistemas basados en IA que utilice para el Tratamiento de Datos Personales, objeto del presente DPA.

(Nota: *Aquellos Sistemas basados en IA, no declarados, se tendrán como no autorizadas por el Responsable, y configurará un incumplimiento contractual. El Encargado deberá previamente informar al Responsable cualquier modificación sobre este numeral y solicitar su autorización expresa).*

Nombre del (los) Sistema(s) basado en IA:	***Completar***
Indicación si se trata de Sistema basado en IA desarrollado por el propio Encargado, Sub-encargado o por un tercero (*precisar*):	
En caso el desarrollo hubiera estado a cargo de un tercero, indique su información de contacto (*razón social, dirección y país*):	
Usos que se le dará al Sistema basado en IA (*precise si los Datos Personales se emplearán sólo para la ejecución del Encargo o se incorporarán al proceso de entrenamiento del Sistema):*	
Indique las medidas con las que cuenta el Sistema basado en IA para garantizar la seguridad de los Datos Personales materia del Encargo y de ser el caso la Subcontratación:	
Indique si cuenta con Políticas, protocolos y/o procedimientos que permitan preservar la seguridad y la protección de los Datos Personales en el uso del (los) Sistemas basados en IA (*precise los documentos con los que cuenta*):	

APÉNDICE 4

ACUERDO MODELO DE TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES ENTRE RESPONSABLE Y ENCARGADO

Las Partes del Contrato de Encargo de Protección de Datos Personales (en adelante, el "Contrato" o "DPA") han acordado el presente Acuerdo basado en cláusulas contractuales modelo (en lo sucesivo, "cláusulas contractuales modelo", "CCM" o "El Acuerdo"):

PARTES DEL ACUERDO:

Exportador de datos

Nombre completo: INTEGRATEL PERÚ S.A.A.

Domicilio: Jirón Domingo Martinez Luján 1130, Surquillo – Lima - Perú

Contacto: Véase el apartado 3.1.2 y 3.1.3 de la tabla del Apéndice 3 del DPA.

Ley Aplicable: Ley 29733 y su Reglamento DS 016-2024-JUS (Perú)

Autoridad de control competente: Autoridad Nacional de Protección de Datos Personales – Perú.

Importador de datos

Nombre completo: Véase el apartado 3.2.1 y 3.2.2 de la tabla del Apéndice 3 – cuestiones generales del tratamiento – del DPA.

Domicilio: Véase los apartados **3.2.3, 3.2.4, y 3.2.5** de la tabla del Apéndice 3 – cuestiones generales del tratamiento – del DPA

Contacto: Véase el apartado 3.2.1 de la tabla del Apéndice 3 – cuestiones generales del tratamiento – del DPA.

PRIMERA PARTE: CUESTIONES GENERALES

Cláusula 1

Finalidad, partes, ámbito de aplicación y definiciones

1.1. **Finalidad**

a. La finalidad de las presentes CCM es garantizar y facilitar el cumplimiento de los requisitos previstos por la Ley Aplicable para la Transferencia internacional de Datos Personales, a fin de cumplir los principios y deberes en la protección de los Datos Personales.
b. Cualquier interpretación del presente Acuerdo deberá tener en cuenta estos fines.

1.2. **Partes del Acuerdo**

c. Las Partes del Acuerdo son el Exportador de datos y el Importador de datos.
d. El presente Acuerdo permite la incorporación de Importadores de datos o Exportadores de datos adicionales como Partes, mediante el formulario del Anexo A siguiendo el procedimiento previsto en la cláusula 5.

1.3. **Ámbito de aplicación**

El presente Acuerdo se aplicará a las Transferencias Internacionales de Datos Personales realizadas entre el Exportador de datos y el Importador de datos de conformidad con las especificaciones del Anexo B. Todos los anexos forman parte del presente Acuerdo.

1.4. **Definiciones**

a. Los términos definidos se identifican en este Acuerdo con sus iniciales en mayúscula.
b. A los fines del presente Acuerdo se entenderá por:

Acuerdo: el presente contrato de Transferencia internacional de Datos Personales basado en las cláusulas contractuales modelo junto con su carátula y sus anexos.

Anonimización: la aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o reidentificación de una persona física sin esfuerzos desproporcionados.

Autoridad de control competente: Autoridad de protección de Datos Personales del país del Exportador o del Importador de Datos Personales.

Computación en la nube: modelo para habilitar el acceso a un conjunto de servicios computacionales (Ej: Redes, servidores, almacenamiento, aplicaciones y servicios) de manera conveniente y por demanda, que pueden ser rápidamente aprovisionados y liberados con un esfuerzo administrativo y una interacción con el proveedor del servicio.

Consentimiento: manifestación de la voluntad, libre, específica, inequívoca e informada, del Titular a través de la cual acepta y autoriza el Tratamiento de los Datos Personales que le conciernen.

Datos Personales: cualquier información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando esto no requiera plazos o actividades desproporcionadas.

Datos Personales sensibles: aquellos que se refieran a la esfera íntima de su Titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los Datos Personales que puedan revelar aspectos como origen racial o étnico, creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física.

Decisiones individuales automatizadas: Decisiones que produzcan efectos jurídicos al Titular o le afecten de manera significativa y que se basen únicamente en tratamientos automatizados destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

Encargado: prestador de servicios que, con el carácter de persona física o jurídica o autoridad pública, ajena a la organización del Responsable, trata Datos Personales a nombre y por cuenta de éste.

Estándares: Estándares de Protección de Datos Personales para los Estados Iberoamericanos aprobados por la RIPD en 2017.

Exportador de datos: persona física o jurídica de carácter privado, autoridad pública, servicios, organismo o prestador de servicios situado en territorio de un Estado que efectúe Transferencias internacionales, conforme a lo dispuesto en las presentes Estándares.

Importador de datos: persona física o jurídica de carácter privado, autoridad pública, servicios, organismo o prestador de servicios situado en un tercer país que recibe Datos Personales de un Exportador de datos mediante una Transferencia internacional.

Ley Aplicable: es la ley de protección de Datos Personales de la jurisdicción del Exportador de datos.

Medidas administrativas, físicas y técnicas: medidas destinadas a evitar el daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los Datos Personales aun cuando ocurra de manera accidental, suficientes para garantizar la confidencialidad, integridad y disponibilidad de los Datos Personales.

Responsable: persona física o jurídica de carácter privado, autoridad pública, servicios u organismo que, solo o en conjunto con otros, determina los fines, medios, alcance y demás cuestiones relacionadas con un tratamiento de Datos Personales.

Subencargado: cuando un Encargado del tratamiento recurre a otro Encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del Responsable.

Terceros beneficiarios: Titular cuyos Datos Personales son objeto de una Transferencia internacional en virtud del presente Acuerdo. El Titular es un tercero beneficiario de los derechos dispuestos en su favor en las CCM y por ende puede ejercer los derechos que las CCM le reconoce, aunque no haya suscripto el contrato modelo entre las partes.

Titular: persona física a quien le conciernen los Datos Personales.

Transferencia ulterior: Transferencia de datos realizada por el Importador de datos a un tercero situados fuera de la jurisdicción del Exportador de datos que cumple las garantías establecidas en las CCM.

Tratamiento: cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizadas sobre Datos Personales, relacionadas, de manera enunciativa más no limitativa, con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de Datos Personales.

Vulneración de la seguridad de Datos Personales: cualquier daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los Datos Personales aun cuando ocurra de manera accidental.

Cláusula 2

Efectos e invariabilidad de las cláusulas

2.1. **Modificación de las cláusulas contractuales modelo. Límites**

El presente Acuerdo basado en cláusulas contractuales modelo establece garantías adecuadas para el Titular en relación con las Transferencias internacionales de Responsables a Encargados, siempre que las Cláusulas no se modifiquen en su esencia respecto al modelo original, salvo para completar la carátula y los anexos. Esto no es óbice para que las Partes incluyan en un contrato más amplio las cláusulas contractuales modelo, ni para que añadan otras cláusulas o garantías adicionales siempre que no contradigan, directa o indirectamente, a las presentes cláusulas contractuales modelo ni perjudiquen los derechos del Titular.

2.2. **Jerarquía con la Ley Aplicable. Interpretación**

a. El presente Acuerdo deberá leerse e interpretarse con arreglo a las disposiciones de la Ley Aplicable.
b. Las Partes podrán añadir nuevas definiciones de términos, resguardos y garantías adicionales en las presentes cláusulas contractuales modelo cuando ello resulte necesario para cumplir con la Ley Aplicable y siempre y cuando ello no suponga un detrimento a las protecciones otorgadas por las cláusulas contractuales modelo.
c. El presente Acuerdo no se podrá interpretar de manera que entre en conflicto con los derechos y obligaciones establecidos en la Ley Aplicable.
d. El presente Acuerdo se entiende sin perjuicio de las obligaciones a las que esté sujeto el Exportador de datos en virtud de su legislación o de la Ley Aplicable.

2.3. **Jerarquía con otros acuerdos**

En caso de contradicción entre el presente Acuerdo y las disposiciones de acuerdos conexos entre las Partes se establece que las cláusulas del presente Acuerdo prevalecerán.

Cláusula 3

Terceros beneficiarios

Los Titulares podrán invocar, como Terceros beneficiarios, las cláusulas del presente Acuerdo contra el Exportador de datos y/o el Importador de datos y exigirles su cumplimiento.

Cláusula 4

Descripción de la transferencia o transferencias, y sus finalidades

Los detalles y características de la transferencia o las transferencias y, en particular, las categorías de Datos Personales que se transfieren y las finalidades para los que se transfieren se detallan en el Anexo B del presente Acuerdo.

Cláusula 5

Cláusula de incorporación

a. Las Partes aceptan que cualquier entidad que no sea parte en el presente Acuerdo podrá, previo consentimiento de todas las Partes intervinientes, adherirse al presente Acuerdo en cualquier momento, ya sea como Exportador de datos o como Importador de datos firmando el modelo del anexo A, y completando los demás Anexos si corresponde.

b. Cuando haya firmado el Anexo A y completado los demás anexos en caso de que corresponda, la entidad que se adhiera se considerará Parte del presente Acuerdo y tendrá los derechos y obligaciones de un Exportador de datos o un Importador de datos, según la categoría en la que se haya adherido al Acuerdo según lo indicado en el Anexo A.

c. La entidad que se sume al Acuerdo no adquirirá derechos y obligaciones del presente Acuerdo derivados del período anterior a su adhesión.

SEGUNDA PARTE: OBLIGACIONES DE LAS PARTES

Cláusula 6

Incumplimiento de las cláusulas y resolución del contrato

6.1. **Instrucciones**

El Importador de datos realizará las actividades de Tratamiento de Datos Personales sin ostentar poder alguno de decisión sobre el alcance y contenido del mismo, así como limitará sus actuaciones a los términos e instrucciones fijados por el Exportador de datos.

6.2. **Principio de responsabilidad**

a. El Exportador de datos garantiza que ha hecho esfuerzos razonables para determinar que el Importador de datos puede, aplicando Medidas administrativas, físicas y técnicas adecuadas, cumplir las obligaciones que le atribuye el presente Acuerdo.
b. El Importador de datos implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en el presente Acuerdo, así como rendirá cuentas sobre el Tratamiento de Datos Personales en su posesión al Titular y a la Autoridad de control competente.
c. El Importador de datos revisará y evaluará permanentemente los mecanismos que para tal afecto adopte voluntariamente para cumplir con el principio de responsabilidad, con el objeto de medir su nivel de eficacia en cuanto al cumplimiento presente Acuerdo.

6.3. **Principio de finalidad**

El Importador de datos no podrá tratar los Datos Personales objeto de este Acuerdo para finalidades distintas a aquéllas indicadas en el Anexo B, salvo cuando siga instrucciones adicionales del Exportador de datos.

6.4. **Transparencia**

a. Previa solicitud, las Partes pondrán gratuitamente a disposición del Titular una copia del presente Acuerdo. En cualquier caso, el Importador de datos asume de oficio la responsabilidad de informar de su existencia. Podrán excluirse aquellas secciones o anexos del Acuerdo que tengan secretos comerciales u otro tipo de información confidencial tales como Datos Personales de terceros o información reservada en términos de la Ley Aplicable.
b. La presente cláusula se entiende sin perjuicio de las obligaciones que la Ley Aplicable atribuyen al Exportador de datos.

6.5. **Exactitud y minimización de datos**

a. Si el Importador de datos tiene conocimiento de que los Datos Personales que ha recibido son inexactos o han quedado obsoletos, informará de ello al Exportador de datos sin dilación indebida.
b. En este caso, el Importador de datos colaborará con el Exportador de datos para suprimir o rectificar los datos.

6.6. **Principio de Seguridad**

a. El Importador de datos y, durante la Transferencia internacional, también el Exportador de datos establecerán y mantendrán Medidas de carácter administrativo, físico y técnico suficientes para garantizar la confidencialidad, integridad y disponibilidad de los Datos Personales objeto de este Acuerdo; en particular, la protección contra Vulneración de la seguridad de Datos Personales. A la hora de determinar un nivel adecuado de seguridad, las partes tendrán debidamente en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del Tratamiento, y los riesgos que entraña el Tratamiento para los Titulares. Al cumplir las obligaciones que le impone el presente párrafo, el Importador de datos aplicará, al menos, las Medidas administrativas, físicas y técnicas que figuran en el Anexo C del presente Acuerdo. El Importador de datos llevará a cabo controles periódicos para garantizar que estas medidas sigan proporcionando un nivel de seguridad adecuado.

b. En caso de Vulneración de la seguridad de Datos Personales tratados por el Importador de datos en virtud del presente Acuerdo, el Importador de datos adoptará medidas adecuadas para ponerle remedio y, en particular, medidas para mitigar los efectos negativos.
c. El Importador de datos también notificará al Exportador de datos de forma inmediata una vez tenga conocimiento de la Vulneración de la seguridad. Dicha notificación incluirá una descripción de la naturaleza de la Vulneración (en la que figuren, cuando sea posible, las categorías y el número aproximado de Titulares y registros de Datos Personales afectados), las consecuencias probables y las medidas adoptadas o propuestas para poner remedio a la Vulneración de la seguridad de Datos Personales, y especialmente, en su caso, medidas para mitigar sus posibles efectos negativos.
d. Cuando y en la medida en que no se pueda proporcionar toda la información al mismo tiempo, en la notificación inicial se proporcionará la información de que se disponga en ese momento y, a medida que se vaya recabando, la información adicional se irá proporcionando sin dilación indebida.
e. El Importador de datos deberá colaborar con el Exportador de datos y ayudarle para que pueda cumplir las obligaciones que le atribuye la Ley Aplicable, especialmente en cuanto a la notificación a la Autoridad de control competente y a los Titulares afectados, teniendo en cuenta la naturaleza del Tratamiento y la información de que disponga el Importador de datos.

6.7. **Tratamiento bajo la autoridad del Importador de datos y principio de confidencialidad**

a. El Importador de datos se asegurará de que las personas que actúen bajo su autoridad solo traten los Datos Personales siguiendo sus instrucciones, y solo concederá acceso a los Datos Personales a los miembros de su personal en la medida en que sea estrictamente necesario para la ejecución, la gestión y el seguimiento del Acuerdo.
b. El Importador de datos garantizará que las personas autorizadas para tratar los Datos Personales mantengan y respeten la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el Exportador de datos.

6.8. **Tratamiento de Datos Personales sensibles**

a. En la medida en que la transferencia incluya Datos Personales sensibles, el Importador de datos aplicará las restricciones específicas y/o las garantías adicionales descritas en el Anexo C de este Acuerdo.
b. En la medida que la transferencia incluya Datos Personales concernientes a niñas, niños y adolescentes, el Importador deberá privilegiar la protección del interés superior de éstos, conforme a la Convención sobre los Derechos del Niño y demás instrumentos internacionales.

6.9. **Transferencias ulteriores**

a. El Importador de datos solo comunicará los Datos Personales a un tercero siguiendo instrucciones documentadas del Exportador de datos.
b. Por otra parte, solo se podrán comunicar los datos a terceros situados fuera de la jurisdicción del Exportador si el tercero está vinculado por el presente Acuerdo o consiente a someterse a este. De no ser así, el Importador de datos solo podrá efectuar una Transferencia ulterior solamente si:

i) Para el caso que la Ley Aplicable así lo disponga, esta Transferencia ulterior va dirigida a un país que ha sido objeto de una declaración de adecuación de su nivel de protección de Datos Personales con arreglo a lo dispuesto en la Ley Aplicable, siempre que tal declaración cubra la Transferencia ulterior;

ii) el tercero destinatario de la Transferencia ulterior aporta de algún modo garantías adecuadas, con arreglo a lo dispuesto en la Ley Aplicable, respecto

a los Datos Personales sujetos a la Transferencia ulterior;

iii) la Transferencia ulterior es necesaria para la formulación, el ejercicio o la defensa de reclamaciones en el marco de procedimientos administrativos, reglamentarios o judiciales específicos;

iv) si es necesario para proteger interess vitales del Titular o de otra persona física.

c. Toda Transferencia ulterior estará sujeta a que el Importador de datos adopte las demás garantías previstas en el presente Acuerdo y, en particular cumpla con el principio de finalidad.

6.10. **Documentación y cumplimiento**

a. Las Partes deberán poder demostrar el cumplimiento de las obligaciones derivadas del presente Acuerdo. En particular, el Importador de datos conservará suficiente documentación de las actividades de tratamiento que se realicen bajo instrucciones del Exportador de datos, que pondrán a disposición del Exportador de datos y de la Autoridad de control competente previa solicitud.
b. El Importador de datos resolverá con presteza y de forma adecuada las consultas del Exportador de datos relacionadas con el Tratamiento con arreglo al presente Acuerdo.
c. El Importador de datos pondrá a disposición del Exportador de datos toda la información necesaria para demostrar el cumplimiento de las obligaciones contempladas en el presente Acuerdo y, a instancia del Exportador de datos, permitirá y contribuirá a la realización de auditorías de las actividades de tratamiento cubiertas por el presente Acuerdo, a intervalos razonables o si existen indicios de incumplimiento. El Exportador de datos podrá optar por realizar la auditoría por sí mismo o autorizar a un auditor independiente. Las auditorías podrán consistir en inspecciones de los locales o instalaciones físicas del importador de datos y, cuando proceda, realizarse con un preaviso razonable.
d. Las Partes pondrán a disposición de la Autoridad de control competente, a instancia de esta, la información a que se refieren los párrafos anteriores y, en particular, los resultados de las auditorías.

6.11. **Duración del Tratamiento y supresión o devolución de los datos**

a. El Tratamiento por parte del Importador de datos solo se realizará durante el período especificado en el Anexo B de este Acuerdo.
b. Una vez se hayan prestado los servicios de Tratamiento, el Importador de datos suprimirá en forma segura, a petición del Exportador de datos, todos los Datos Personales tratados por cuenta del Exportador de datos y acreditará al Exportador de datos que lo ha hecho, o devolverá al Exportador de datos todos los datos y suprimirá de forma segura las copias existentes, si el Exportador de datos optare por esta última opción. Hasta que se destruyan o devuelvan los Datos Personales, el Importador de datos seguirá garantizando el cumplimiento con el presente Acuerdo. Si el derecho del país aplicable al Importador de datos prohíbe la devolución o la destrucción de los Datos Personales, el Importador de datos se compromete a seguir garantizando el cumplimiento del presente Acuerdo y solo tratará los datos en la medida y durante el tiempo que exija el derecho del país del Importador de datos.

Cláusula 7

Recurso a sub-encargados

7.1. **Forma de autorización del Sub-encargado**

AUTORIZACIÓN GENERAL POR ESCRITO:

El Importador de datos cuenta con una autorización general del Exportador de datos para contratar a Sub-encargados que figuren en una lista acordada. El Importador de datos informará al Exportador de datos específicamente y por escrito de las adiciones o sustituciones de Sub-encargados previstas en dicha lista con antelación, de modo que el Exportador de datos tenga tiempo suficiente para formular una objeción a tales cambios dentro de los diez (10) días calendario siguientes a su notificación y antes de que se contrate al Sub-encargado o Sub-encargados de que se trate. El Importador de datos proporcionará al Exportador de datos la información necesaria para que este pueda ejercer su derecho a formular objeciones.

7.2. **Contrato con el Sub-encargado**

a. Cuando el Importador de datos recurra a un Sub-encargado para llevar a cabo actividades específicas de tratamiento (por cuenta del Exportador de datos), lo hará por medio de un contrato escrito que establezca, en esencia, las mismas obligaciones en materia de protección de datos que las impuestas al Importador de datos en virtud del presente Acuerdo, especialmente en lo que se refiere a los derechos de los Titulares en cuanto sean Terceros beneficiarios. Las Partes convienen que, al cumplir el presente Acuerdo, el Importador de datos también da cumplimiento a las obligaciones que le atribuye la cláusula relativa a Transferencias ulteriores. El Importador de datos se asegurará de que el Sub-encargado cumpla las obligaciones que le atribuya el presente Acuerdo.
b. El Importador de datos proporcionará al Exportador de datos, a instancia de este, una copia del contrato con el Sub-encargado y de cualquier modificación posterior del mismo. En la medida en que sea necesario para proteger información confidencial, como Datos Personales, el Importador de datos podrá proteger esa información antes de compartir la copia.
c. El Importador de datos seguirá siendo plenamente responsable ante el Exportador de datos del cumplimiento de las obligaciones que imponga al Sub-encargado su contrato con el Importador de datos. El Importador de datos notificará al Exportador de datos los incumplimientos por parte del Sub-encargado de las obligaciones que le atribuye dicho contrato.

Cláusula 8.

Derechos de los Titulares

a. El Importador de datos notificará con presteza al Exportador de datos las solicitudes que reciba del Titular. No responderá a dicha solicitud por sí mismo, a menos que el Exportador de datos le haya autorizado.
b. El Importador de datos ayudará al Exportador de datos a cumplir sus obligaciones al responder a las solicitudes de ejercicio de derechos que la Ley Aplicable atribuye a los Titulares. A este respecto, las Partes establecerán en el anexo C sobre Medidas administrativas, físicas y técnicas apropiadas, teniendo en cuenta la naturaleza del Tratamiento, por las que se garantice que se prestará ayuda al Exportador a aplicar la presente cláusula, así como el objeto y el alcance de la ayuda requerida.
c. En el cumplimiento de las obligaciones que le atribuyen los dos párrafos anteriores, el Importador de datos seguirá las instrucciones del Exportador de datos.

Cláusula 9

Reclamaciones

a. El Importador de datos informará a los Titulares, de forma transparente y en un formato de fácil acceso, mediante notificación individual o en su página web, del punto de contacto autorizado para tramitar reclamaciones. Este tramitará las reclamaciones que reciba de los Titulares con la mayor brevedad.
b. En caso de litigio entre un Titular y una de las Partes en relación con el cumplimiento del presente Acuerdo, dicha parte hará todo lo posible para resolver amistosamente el problema de forma oportuna. Las Partes se mantendrán mutuamente informadas de tales litigios y, cuando proceda, colaborarán de buena fe para resolverlos.
c. El Importador de datos se compromete a aceptar y no controvertir, cuando el Titular invoque un derecho de Tercero Beneficiario que deriven de este Acuerdo, la decisión del Titular de: (i) presentar una reclamación ante la autoridad de control de datos del Estado de su residencia habitual o su lugar de trabajo o ante la Autoridad de control competente; (ii) ejercitar una acción judicial sobre sus Datos Personales.
d. El Importador de datos acepta acatar las resoluciones que sean vinculantes con arreglo a la Ley Aplicable o el derecho de que se trate.

Cláusula 10

Responsabilidad civil

a. Cada parte será responsable ante la(s) otra(s) de cualquier daño y perjuicio que le(s) cause por cualquier vulneración del presente Acuerdo.
b. El Importador de datos será responsable ante el Titular. El Titular tendrá derecho a que se le indemnice por los daños y perjuicios materiales o inmateriales que el Importador de datos o su Sub-encargado ocasionen al Titular por vulnerar los derechos de Terceros beneficiarios que deriven del presente Acuerdo. Lo anterior se entiende sin perjuicio de la responsabilidad del Exportador de datos con arreglo a la Ley Aplicable.
c. Las Partes acuerdan que, si el Exportador de datos es considerado responsable, de conformidad el párrafo anterior, de los daños o perjuicios causados por el Importador de datos (o su Sub-encargado), estará legitimado para exigir al Importador de datos la parte de la indemnización que sea responsabilidad del Importador de los datos.
d. Cuando más de una Parte sea responsable de un daño o perjuicio ocasionado al Titular como consecuencia de una vulneración del presente Acuerdo, todas las Partes responsables serán responsables solidariamente.
e. Las Partes acuerdan que, si una parte es considerada responsable con arreglo al párrafo anterior estará legitimada para exigir a la otra Parte la parte de la indemnización correspondiente a su responsabilidad por el daño o perjuicio.
f. El Importador de datos no puede alegar la conducta de un Sub-encargado del tratamiento para eludir su propia responsabilidad.

Cláusula 11

Supervisión de la Autoridad competente

a. El Importador de datos acepta someterse a la jurisdicción de la Autoridad de control competente y a cooperar con ella en cualquier procedimiento destinado a garantizar el cumplimiento del presente Acuerdo.
b. En particular, el Importador de datos se compromete a responder a consultas, someterse a auditorías y cumplir las medidas adoptadas por la Autoridad de control y, en particular, las medidas correctivas e indemnizatorias. Remitirá a la Autoridad de control confirmación por escrito de que se han tomado las medidas necesarias.

Cláusula 12

Derecho y prácticas del país que afectan al cumplimiento de las cláusulas

a. Las Partes confirman que, al momento de celebrar este Acuerdo, han realizado esfuerzos razonables para identificar si los datos transferidos están cubiertos por alguna ley o práctica local de la jurisdicción del Importador de datos que va más allá de lo que es necesario y proporcional en una sociedad democrática para salvaguardar importantes objetivos de interés público y puede razonablemente esperarse que afecte las protecciones, derechos y garantías otorgadas bajo este Acuerdo al Titular. En base a lo expuesto las Partes confirman que no están al tanto que dicha práctica o norma exista o afecte adversamente las protecciones específicas bajo este Acuerdo.
b. El Importador de datos se compromete a notificar en forma inmediata al Exportador de datos si alguna de estas leyes se le aplica en el futuro. De realizarse dicha notificación o si el Exportador de datos tiene motivos para creer que el Importador de datos ya no puede cumplir con las obligaciones de este Acuerdo, el Exportador de datos identificará las medidas apropiadas (por ejemplo, Medidas administrativas, físicas y técnicas para garantizar la seguridad) para remediar la situación. Asimismo, podrá suspender las transferencias objeto de este Acuerdo si considera que no pueden asegurarse las garantías adecuadas. En este caso, el Exportador de datos tendrá derecho a rescindir este Acuerdo de conformidad con lo dispuesto en la cláusula 13.
c. Si un tribunal o una agencia gubernamental requiere que el Importador de datos divulgue o utilice los datos transferidos de una manera que de otro modo no estaría permitida por este Acuerdo, el Importador de datos revisará la legalidad de dicha solicitud y la impugnará si, después de una evaluación legal cuidadosa, concluye que existen motivos razonables para considerar que la solicitud es ilegal según la legislación local y afecta los derechos garantizados por este Acuerdo. En la medida en que esto esté permitido por la ley local, también deberá informar de inmediato al Exportador de datos que ha recibido dicha solicitud. Si el Importador de datos tiene prohibido notificar al Exportador de datos según la ley local, hará todo lo posible para obtener una exención de la prohibición.

TERCERA PARTE:

DISPOSICIONES FINALES

Cláusula 13.

Incumplimiento de las cláusulas y resolución del contrato

a. El Importador de datos informará inmediatamente al Exportador de datos en caso de que no pueda dar cumplimiento a alguna de las cláusulas de este Acuerdo por cualquier motivo.
b. En caso de que el Importador de datos incumpla las obligaciones que le atribuye el presente Acuerdo, el Exportador de datos suspenderá la Transferencia internacional al Importador de datos hasta que se vuelva a garantizar el cumplimiento o se resuelva el contrato.
c. El Exportador de datos estará facultado para resolver este Acuerdo cuando:

i) el Exportador de datos haya suspendido la Transferencia internacional al Importador de datos con arreglo al párrafo anterior y no se vuelva a dar cumplimiento al presente Acuerdo en un plazo razonable y, en cualquier caso, en un plazo de treinta (30) días hábiles a contar desde la suspensión;
ii) el Importador de datos vulnere de manera sustancial o persistente el presente Acuerdo; o
iii) el Importador de datos incumpla una resolución vinculante de un órgano jurisdiccional o Autoridad de control competente en relación con las obligaciones que le atribuye el presente Acuerdo. En este supuesto, informará a la Autoridad de control competente de su incumplimiento.

d. Los Datos Personales que se hayan transferido antes de la resolución del contrato deberán, a elección del Exportador de datos, devolverse inmediatamente al Exportador de datos o destruirse en su totalidad. Lo mismo será de aplicación a las copias de los datos.

   El Importador de datos acreditará la destrucción de los datos al Exportador de datos. Hasta que se destruyan o devuelvan los datos, el Importador de datos seguirá garantizando el cumplimiento con el presente Acuerdo. Si el derecho del país aplicable al Importador de datos prohíbe la devolución o la destrucción de los Datos Personales transferidos, el Importador de datos se compromete a seguir garantizando el cumplimiento del presente Acuerdo y solo tratará los datos en la medida y durante el tiempo que exija el derecho del país.

Cláusula 14

Derecho aplicable

El presente Acuerdo se regirá por la Ley Aplicable: Ley N° 29733 – Ley de Protección de Datos Personales – Perú y su Reglamento aprobado mediante D.S.0 016-2024-JUS

Cláusula 15

Elección del foro y jurisdicción

a. Cualquier controversia derivada del presente Acuerdo será resuelta judicialmente en los tribunales de la jurisdicción del Exportador de datos.
b. Los Titulares también podrán ejercer acciones judiciales contra el Exportador de datos y/o el Importador de datos, las que podrán ser iniciadas, a elección del Titular, en el país del Exportador de datos, o en el que el Titular tenga su residencia. Con respecto al Importador de datos, también podrán ejercer acciones judiciales en el país del Importador de datos.
c. Las Partes acuerdan someterse a la jurisdicción prevista en esta cláusula.

ANEXOS

ANEXO A: Descripción de la transferencia

ANEXO B: Medias administrativas, físicas, y técnicas para garantizar la seguridad de los datos.

ANEXO C: Lista de Sub-encargados del tratamiento.

Firma del Exportador (Responsable)

Nombre:	
Cargo:	

Firma del Importador (Encargado)

Nombre:	
Cargo:	

ANEXO A

DESCRIPCIÓN DE LA TRANSFERENCIA

Categorías de Titulares cuyos Datos Personales se transfieren: Véase el apartado 3.1.7 del Apéndice 3 – cuestiones generales del tratamiento - del DPA.

Categorías de Datos Personales transferidos: Véase el apartado 3.1.6 del Apéndice 3 – cuestiones generales del tratamiento – del DPA.

Datos Personales sensibles transferidos (si procede) y restricciones o garantías aplicadas: Véase el apartado 3.1.6 del Apéndice 3 – cuestiones generales del tratamiento - del DPA.

Frecuencia de la transferencia: de forma periódica o, en su caso de acuerdo con lo establecido en el apartado 3.1.1 del Apéndice 3 del DPA.

Finalidad(es) de la transferencia y posterior tratamiento de los datos: Véase el apartado 3.1.1 del Apéndice 3 – cuestiones generales del tratamiento - del DPA.

Plazo: Véase el apartado 3.1.8 del Apéndice 3 – cuestiones generales del tratamiento - del DPA.

Subencargados: Véase el apartado 3.3 del Apéndice 3 – cuestiones generales del tratamiento - del DPA.

ANEXO B

MEDIDAS ADMINISTRATIVAS, FISICAS Y TÉCNICAS PARA GARANTIZAR LA SEGURIDAD DE LOS DATOS

Aplica el Apéndice 1 del DPA.

ANEXO C

LISTA DE SUB-ENCARGADOS DEL TRATAMIENTO

Aplica el apartado 3.3. del Apéndice 3 del DPA.

ANEXO 8

DECLARACIÓN JURADA
Devolución / Supresión de Información (Datos Personales)

Mediante el presente documento, _____ con RUC N° _____debidamente representada por _____, identificado con DNI N°_____, (en adelante, el “Proveedor” o el "Encargado del Tratamiento”), declara lo siguiente:

1. Con fecha XX/XX/XXXX, el Encargado del Tratamiento e Integratel Perú S.A.A. (en adelante, "Integratel") celebraron el Contrato de Prestación de Servicios de _____ (en adelante, el "Contrato").

2. Integratel en su condición de Responsable del Tratamiento, encargó el Tratamiento de Datos Personales al Proveedor, razón por el cual las partes suscribieron un DPA[12] que se anexó al Contrato.

3. Debido a que el plazo del Contrato llegó a su término, en cumplimiento de la cláusula 4.4 del DPA suscrito, el Encargado hace entrega a Integratel de los Datos Personales recibidos y cuyo detalle se anexa al presente documento.

4. En caso resulte materialmente imposible la devolución de los Datos Personales a Integratel, o las partes así lo acuerdan, el Encargado suscribe presente certificación en calidad de Declaración Jurada asegurando que ha cumplido con la supresión segura de los Datos Personales tratados por encargo de Integratel.

5. El Encargado se obliga a mantener indemne a Integratel, respondiendo toda demanda, acción o reclamación, ya sea administrativa o judicial, que pudiera ser interpuesta contra el Integratel, como consecuencia del incumplimiento de la obligación establecida en el presente documento, quien se compromete a seguir el procedimiento correspondiente conforme a derecho, a efectos de defender a Integratel. Si a pesar de lo anterior, cualquier autoridad o titular afectado imputara responsabilidad a Integratel y se decidiera por la autoridad competente la imposición de sanciones pecuniarias o indemnizaciones, éstas serán asumidas por el Encargado, o si fueran pagadas por Integratel, serán reembolsadas por el Encargado, sin perjuicio de la responsabilidad que pudiera corresponderle por cualquier daño y/o perjuicio ulterior causado a Integratel.

En señal de conformidad con lo establecido en el presente documento, ambas partes suscriben el mismo en el lugar y fecha que se señala.

Lima, ___ de _____ del ____

_____

El Encargado (Proveedor)

[12] DPA o Contrato de Encargo para el Tratamiento de Datos Personales.