I. OBJETIVO:

Dar a conocer las exigencias de la Ley de Protección de Datos Personales (Ley Nº 29733) y su Reglamento a todos los colaboradores de la compañía, así como garantizar su cumplimiento.

II. ALCANCE:

Todos aquellos procesos que involucren información de datos personales de los colaboradores, clientes, proveedores de servicios y terceros de **ESIGTEK DEL PERÚ S.A.C**., en adelante, **ESIGTEK**.

III. DEFINICIONES:

- **APDP:** Autoridad Nacional de Protección de Datos Personales.
- **Autorización:** conocimiento previo e informado del titular del dato para llevar a cabo el tratamiento de sus datos personales.
- **Aviso de Privacidad:** Comunicación verbal o escrita generada por el Titular del Banco de Datos Personales, dirigida al Titular de los Datos Personales informando el tratamiento sus datos personales.
- **Banco de Datos Personales:** Conjunto organizado de datos personales, automatizado o no, que cuenta con una determinada finalidad, cualquiera que sea la forma de su creación, formación, almacenamiento, organización y acceso; pudiendo inclusive pertenecer los mismos datos personales a más de un banco de datos personales.
- **Banco de Datos Personales No Automatizado:** conjunto de datos de personas naturales no computarizado, y estructurado conforme a criterios específicos, que permita acceder, sin esfuerzos desproporcionados, a los datos personales.
- **Bloqueo:** es la medida por la que el encargado del banco de datos personales impide el acceso de terceros a los datos y éstos no pueden ser objeto de tratamiento, durante el período de bloqueo.
- **Cancelación:** es la acción o medida, que en la Ley se describe como “supresión”, cuando se refiere a datos personales, que consiste en eliminar o suprimir los datos personales de un banco de datos.
- **Datos Personales:** toda aquella información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables.
- **Datos personales relacionados con la salud:** es aquella información concerniente a la salud pasada, presente o pronosticada, física o mental, de una persona, incluyendo el grado de discapacidad y su información genética.
- **Dato público:** es aquel dato que no es semiprivado, privado o sensible.
- **Datos indispensables:** son aquellos datos personales de los titulares, que son obligatorios para poder iniciar o mantener una relación jurídica con la empresa.
- **Datos opcionales:** son aquellos datos que La Empresa requiere para ofrecer servicios adicionales.

- **Datos sensibles:** datos personales referidos al origen racial o étnico de una persona, ingresos económicos, datos relacionados a la salud, opiniones o convicciones políticas, religiosas, filosóficas o morales, afiliación sindical, e información relacionada a la salud, a la vida sexual, entre otros.
- **Derechos ARCO:** Derecho de Actualización, Derecho de rectificación, Derecho de Cancelación y Derecho de Oposición.
- **Encargado del Tratamiento:** Persona Natural o Jurídica, pública o privada que por sí misma o en asociación por otros, realice el tratamiento de datos personales en nombre del responsable del tratamiento.
- **Flujo Transfronterizo de datos personales:** transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban.
- **Hábeas Data:** derecho de cualquier persona a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en el banco de datos y en archivos de entidades públicas y privadas.
- **Procedimiento de anonimización:** tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible.
- **Procedimiento de disociación:** tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es reversible.
- **Rectificación:** es aquella acción genérica destinada a afectar o modificar un banco de datos personales ya sea para actualizarlo, incluir información en él o específicamente corregir sus contenidos con datos exactos.
- **Responsable del Banco de Datos Personales:** persona encargada de cada banco de datos personales, y del cumplimiento de las exigencias de la ley sobre el mismo.
- Responsable del Tratamiento: es aquel que decide sobre el tratamiento de datos personales.
- **Titular de Datos Personales:** persona natural a quien corresponde los datos personales.
- **Titular del Banco de Datos Personales:** determinada la finalidad y contenido de los bancos de datos personales, el tratamiento de estos y las medidas de seguridad (La Empresa).
- **Tratamiento de datos personales:** cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquiera otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.
- **Transferencia de datos personales:** toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales.

IV. PRINCIPIOS RECTORES:

ESIGTEK, en su calidad de Titular del Banco de Datos Personales deben cumplir con los principios rectores de la protección de datos personales de conformidad con lo establecido en las normas de Protección de Datos Personales:

a) **Principio de Legalidad:** el tratamiento de los datos personales se hace conforme a lo establecido en la Ley. Se prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos.

b) Principio de Consentimiento: para el tratamiento de los datos personales, debe mediar el consentimiento del titular de manera expresa ya sea por medios escritos **y/o digitales.**

c) **Principio de Finalidad:** Se considera que una finalidad está determinada, cuando haya sido expresada con claridad, sin lugar a confusión y cunado de manera objetiva se especifica el objeto que tendrá el Tratamiento de los Datos Personales, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización.

d) **Principio de Proporcionalidad:** Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.

e) **Principio de Calidad:** los Datos Personales contenidos en un Banco de Datos Personales deben ajustarse con precisión a la realidad. Se presume que los datos directamente facilitados por el Titular de los mismos son exactos. Deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario

f) **Principio de Seguridad:** En el Tratamiento de los Datos Personales deben adoptarse las medidas de seguridad que resulten necesarios a fin de evitar cualquier tratamiento contrario a las Normas de Protección de Datos Personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales que se trate.

g) **Principio de Disposición de Recurso:** todo Titular de Datos Personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerables por el tratamiento de sus datos personales.

h) **Principio de Nivel de Protección Adecuado:** Para el flujo transfonterizos de datos personales, se debe garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar o por lo menos, equiparable a lo previsto por las normas de Protección de Datos Personales o por lo estándares internacionales en la materia.

V. RESPONSABILIDADES:

Gobierno de Datos:

- Inscribir los bancos de datos personales y mantenerlos actualizados ante la Autoridad Nacional de Datos Personales.

- Inscribir la transferencia de información transfronteriza.
- Mantener actualizada la Política de Protección de Datos Personales de acuerdo a los objetivos estratégicos del negocio, la legislación y la norma vigente y coordinar su publicación y difusión.
- Definir los cargos de los Bancos/Sub Bancos de datos que gestiona la compañía.
- Proporcionar la información relativa al tratamiento de datos personales a la Autoridad Nacional de Protección de Datos Personales cuando ésta lo requiera, asimismo permitirle el acceso a los bancos de datos personales que la compañía administra.
- Guardar toda la información respecto a la solicitud de los derechos ARCO en medios físicos y/o digitales.

Seguridad de la Información:

- Cumple el rol de Representante de seguridad de los bancos de datos personales, por el cual será responsable de:
  a) Velar que la Política de Protección de Datos Personales esté alineada de acuerdo a los objetivos estratégicos del negocio, la legislación y la normativa vigente.
  b) Coordinar el cumplimiento e implementación de los controles de seguridad necesarios, en coordinación con las áreas de negocio y tecnología, definidos en la presente política.
  c) Revisar periódicamente la efectividad de los controles de seguridad adoptados para la protección de los bancos de datos personales y generar acciones de mejora.

Áreas de negocio y tecnología:

- Implementar controles de seguridad definidos en la presenta Política en coordinación con las áreas de soporte y gestión de riesgos.

Colaboradores:

- Cumplir la presente política y los procedimientos que de ésta deriven.
- Notificar cualquier incidente que comprometa la privacidad de la información de nuestros clientes o a cualquier mal uso de la información que pueda afectar al cliente o la reputación de la compañía.

Asesor Legal:

- Bridar asesoría legal a las distintas áreas de la compañía en cuanto a la absolución de consultas sobre las especificaciones exigidas por la Ley de Protección de Datos Personales y su Reglamento.

Responsable del Banco de Datos Personales:

- Brindar los recursos y dirección en la protección de los datos personales.

Encargado del Banco/ Sub Banco de datos personales:

- Informar a la Unidad de Gobierno de Datos sobre las modificaciones (captura de nuevos datos personales, eliminación y/o modificación de datos personales ya existentes, procesos de anonimización, entre otros) en los bancos de datos personales a fin que se formalicen los cambios con la Autoridad competente.
- Velar por el cumplimiento de la presente política en materia de protección de datos personales de la empresa.
- Autorizar la transferencia de la información de los datos personales, asignados en los bancos, a terceros.
- Asegurar la formalización contractual respecto de la transferencia de la información de datos personales, cuando se realice.
- Responder ante la consulta de una solicitante de los derechos ARCO del banco de datos / sub banco de datos, que le compete.

VI. DESARROLLO DE LA POLÍTICA:

ORGANIZACIÓN ADMINISTRATIVA:

1. La compañía debe definir a los responsables y encargados de cada banco / sub banco de datos personales, los cuales tendrán responsabilidad directa y velarán por el cumplimiento de la presente política.
2. El Titular de los Bancos de Datos es la ESIGTEK, como persona jurídica.
3. El representante de los bancos de datos es la Gerencia General de ESIGTEK.

GESTIÓN Y TRATAMIENTO DE LOS BANCOS DE DATOS PERSONALES:

4. La creación, actualización o suspensión de los bancos de datos debe considerar:
   a) La implementación de procedimientos para la creación, actualización, eliminación y transferencia de banco de datos personales.
   b) La creación de banco de datos personales requiere de la implementación previa de los controles de seguridad necesarios para el cumplimiento de la presente Política, la Ley Nº 29733 y sus normas complementarias.
   c) La creación de banco de datos, su modificatoria y/o los mecanismos de captación de datos personales deben ser aprobados previamente por la Gerencia del Gobierno de Datos que se encuentra a cargo de la Gerencia General.

5. La obtención de datos personales y el consentimiento del titular de datos personales, debe considerar:
   a) La compañía prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos.
   b) Previo a cualquier tratamiento de datos personales, el encargado de cada banco de datos tiene la capacidad de garantizar que se cuente con el consentimiento del titular de datos personales.
   c) Previo a la captura de los datos personales, se debe contar con el consentimiento del titular, el cual debe ser informado expresa e inequívocamente, ya sea por medios físicos o digitales.

d) La recopilación de datos personales para la plataforma ESIGTEK, se realizará a través de la suscripción de un acuerdo comercial con el cliente, quien tendrá la obligación de informar del tratamiento de los datos personales a los titulares de datos personales. Asimismo, ESIGTEK obtendrá la autorización para el tratamiento de los datos personales del titular de datos, a través de su plataforma digital.

e) La recopilación de datos personales debe ser necesaria y lícita con relación a las finalidades determinadas. Asimismo, se debe garantizar la calidad de los datos contenidos en el banco de datos personales, y aplicar las medidas de seguridad necesarias que ayuden a prevenir la adulteración, pérdida y desviación de datos personales.

f) En caso de necesitar efectuar el tratamiento de datos personales de un menor de edad, se requerirá contar con el consentimiento de los padres o tutores de los mismos, según corresponda salvo excepciones previstas en la Ley y su Reglamento. En caso de personas mayores de 14 años no será necesario el consentimiento expreso de los padres o tutores en caso se trate de datos aprobados por la norma.

g) No será necesario el consentimiento cuando los datos de carácter personal:
   - Se recojan para el ejercicio de las funciones propias de ESIGTEK en el ámbito de sus competencias, sea contractual, pre contractual, laboral, negociación y profesional, cuando los datos figuren en fuentes de acceso público o cuando existan excepciones establecidas por la Ley Nº 29733, sus modificatorias y sus normas complementarias.
   - Cuando se realicen actividades de disociación o anonimización.

h) En caso de obtener datos personales sin el previo consentimiento del titular del dato y no exista excepción para su solicitud, se deberán implementar medidas para obtener el consentimiento para tratarlos. Asimismo, se puede obtener el primer contacto con el cliente, siempre y cuando la primera acción sea requerir el consentimiento para contactarlo.

6. La transferencia de datos personales debe considerar:

a) Los encargados de cada banco/sub banco deberán asegurarse de que toda transferencia de datos personales cuente con el consentimiento de su titular, salvo excepciones previstas en la Ley y su Reglamento.

b) Toda transferencia de datos personales, tanto a nivel nacional e internacional, procederá con autorización de cada encargado de banco/sub banco de datos personales, y en el medio por el cual se llevará a cabo dicha transferencia de datos deberá cumplir con la política de seguridad de la información vigente. En caso sea necesario efectuar un flujo transfronterizo de datos personales, los responsables de cada banco de datos deberán garantizar que el país destinatario mantenga los niveles de protección adecuados.

7. La contratación de terceros que efectúan un tratamiento de datos personales debe considerar:

   a) Todo tercero con quien **ESIGTEK** comparta información de datos personales, deberá considerar y cumplir, como parte del servicio vigente, con las exigencias de la Ley de Protección de Datos Personales y su reglamento y/o estándares internacionales en materia de Protección de Datos Personales, lo cual deberá constar en cualquier medio ya se físico o digital.
   b) Será de responsabilidad de cada área, la regularización de los contratos vigentes con terceros mediante la inclusión de las adendas necesarias que contemplen los términos de la Ley. De ser el caso, el asesor legal de **ESIGTEK**, brindará, a solicitud, el asesoramiento de los responsables de las áreas correspondientes en cuanto a los términos tratados y definidos en el contrato.

EJERCICIO DE DERECHOS DEL TITULAR DE DATOS PERSONALES:

8. Se deben almacenar los datos personales de manera que se posibilite el ejercicio de los derechos de su titular.

9. Se deben implementar mecanismos para que el Titular de los datos o los representantes de menores de edad, formulen solicitudes respecto a:

Derecho de la Información:

- Finalidad para la que sus datos serán tratados.
- Quienes son o pueden ser sus destinatarios.
- Identidad y domicilio del Titular del Banco de Datos Personales.
- La transferencia de los datos personales.
- Las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo.
- Tiempo de conservación de los datos.

Derecho de Acceso:

- Obtener la información, de manera gratuita, que sobre sí mismo sea objeto de tratamiento en banco de datos.
- La forma en que sus datos fueron recopilados.
- Razones que motivaron su recopilación.
- A solicitud de quién se realizó la recopilación.
- Transferencias realizadas o que se prevén hacer.

Derecho de Rectificación, Cancelación y Oposición:

- Cuando se hubiera advertido omisión, error o falsedad.
- Cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados. Cuando hubiera vencido el plazo establecido para su tratamiento.

- **ESIGTEK** se reserva el derecho de mantener la información a fin de dar cumplimiento a normas especiales de prevención de lavado de activos.
- Toda solicitud de rectificación debe ser acompañada de la documentación sustentatoria correspondiente.

10. El titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de rectificación, cancelación u oposición, o cuando advierten el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley Nº 29733, podrán presentar una solicitud al Titular del Banco de Datos Personales o al responsable del Tratamiento de **ESIGTEK**, la cual deberá contar con la siguiente información:

    - Nombres y apellidos del titular del derecho y acreditación de los mismos, y en el caso de su representante adjuntando la copia de su documento de identidad y una carta poder legalizada.
    - Petición concreta que da lugar a la solicitud.
    - Dirección, real o electrónica, a efectos de las notificaciones que correspondan.
    - Fecha y firma del solicitante.
    - Documentos que sustenten la solicitud, de ser el caso.

11. El titular o sus causahabientes tienen derecho a presentar ante **ESIGTEK**, consultas y/o reclamaciones previa verificación de su identidad, a través de cualquiera de los siguientes medios.

    - Por escrito: mediante carta dirigida a Calle Loma Rica Nº 296, interior 501, Santiago de Surco.
    - Al correo: soporte@esigtek.com
    - Línea de atención al cliente: 946 286 477

12. Los procedimientos de atención, cualquiera que sea el medio (escrito o telefónico), se debe guardar prueba de la consulta y su respuesta. Asimismo, los reclamos realizados, respecto al tratamiento de datos personales debe ser informado a la Unidad de Seguridad de la Información para la coordinación de los planes de acción correctivos.

13. La atención de las solicitudes y reclamos, por parte de los titulares de los datos personales, debe considerar los siguientes plazos:

Solicitud	Tiempo de Atención
Información	05 días hábiles contados desde el día siguiente de la presentación de la solicitud
Acceso	10 días hábiles contados desde el día siguiente de la presentación de la solicitud
Rectificación, Cancelación, Oposición	10 días hábiles contados desde el día siguiente de la presentación de la solicitud
Tutela de Derechos (APDP)	15 días hábiles contados desde la notificación de la solicitud por parte de la APDP (Autoridad de Protección de Datos Personales)

14. El Titular o causahabientes sólo podrán elevar queja ante la Autoridad Nacional de Protección de Datos Personales, una vez hayan agotado el trámite de consulta o reclamo ante **ESIGTEK**.

DEBERES DE LOS COLABORADORES:

15. Uso inaceptable de la información referida a datos personales:

Las siguientes actividades están prohibidas y se consideran como un uso inaceptable de la información referida a datos personales. La lista es un intento de proporcionar un marco para las actividades que caen en la categoría de uso inaceptable, pero no se limita a:

a) Usar o tratar la información para beneficio propio o de terceros y sin la autorización del titular de la información.
b) Usar la información de datos personales para realizar actividades contrarias a la legislación vigente.
c) Compartir, con otros trabajadores y/o terceros, de manera directa o indirecta la información de datos personales sin la autorización previa de los encargados de los bancos/sub bancos de datos e incumpliendo las políticas establecidas en el presente documento.
d) Ceder directa o indirectamente la información confidencial a terceros, sin la autorización debida de parte de **ESIGTEK**.
e) Recopilar datos personales mediante la realización de fraudes, engaños y de medios no permitidos por la legislación peruana.

16. Deber de secreto y de confidencialidad:

Todo trabajador y/o tercero que intervenga en cualquier fase del tratamiento de los datos personales está obligado a mantener la confidencialidad y el secreto profesional, cuando corresponda, de manera indefinida.

SEGURIDAD DEL BANCO DE DATOS:

17. Gestión de la Seguridad de la Información de Banco de Datos:

a) Los datos personales recopilados por **ESIGTEK** debe ser considerada como información confidencial.
b) La protección de los datos personales se debe incorporar dentro del Sistema de Gestión de Seguridad de la Información a fin de asegurar el cumplimiento de las medidas de control necesarias en cumplimiento con la normativa vigente.

18. Medidas de Seguridad Técnica en el Uso de Tecnologías de información y comunicación (TIC):

    a) El uso de tecnologías de la información como: Bases de Datos, Aplicaciones de negocio, Equipos de Comunicación, Servidores, Sistemas Operativos, entre otros; que soportan la gestión del tratamiento de datos personales, deben implementar los controles de seguridad requeridos en la Ley Nº 29733 (Tipo Complejo) y definidos en la Política de Seguridad de la Información de **ESIGTEK**.

19. Medidas de Seguridad Física para la protección de datos personales:

    ESIGTEK no emplea banco de datos físicos sino digitales; no obstante, si en futuro los tuviese, se aplicarán las siguientes medidas:

    a) Para banco de datos con información sensible, el almacenamiento de información en formato físico debe considerar ubicar el banco de datos personales en un ambiente aislado protegido por cerradura o mecanismo similar, donde la responsabilidad el mecanismo de acceso recae en el Área Usuaria.
    b) Para banco de datos con información no sensible: la información física se debe considerar: Ubicar el banco de datos personales en un gabinete, caja, cajón de un mueble, gaveta o similar, siempre y cuando tenga una cerradura con llave o similar, la cual será responsabilidad del área usuaria.

CAPACITACIÓN Y MONITOREO EN LA PROTECCIÓN DE DATOS PERSONALES:

20. Gestión de Incidentes:
    a) La gestión de incidentes que comprometen datos personales deben ser incluidos dentro del procedimiento de gestión de incidentes de **ESIGTEK**.

21. Auditoría:
    Se debe desarrollar un programa de autoría respecto de cumplimiento, para asegurar la mitigación de los riesgos relacionados a la protección de datos personales. Esta actividad se debe desarrollar como mínimo una vez al año.

22. Capacitación y Compromiso:
    El programa de creación de conciencia y entrenamiento para la protección de datos personales debe ser incorporado dentro del programa de entrenamiento de **ESIGTEK**.

VII. GENERALES:

23. Actualización de la Política:
    a) La Unidad de Seguridad de la Información es responsable de garantizar que la política se mantenga actualizada y sea apropiada a las necesidades de la empresa. La periodicidad para su revisión, actualización o ratificación es cada 2 años, o cuando ocurran cambios significativos en los procesos internos o en la normativa externa.
    b) Cada actualización del documento deberá ser acompañado de la respectiva notificación y capacitación a los obligados de cumplirla y de conocerla.

24. Excepciones y Sanciones:
    a) Cualquier excepción de la presente política debe ser notificado a la Unidad de Seguridad de la Información para su registro y evaluación.
    b) El incumplimiento del presente documento se considerará como falta grave y será sancionado como tal según el reglamento interno de trabajo.
    c) El incumplimiento del presente documento será sancionado de conformidad con lo previsto en le Reglamento Interno de Trabajo.