POLITICA (CÓDIGO DE CONDUCTA) DE PROTECCIÓN DE DATOS PERSONALES

CODIGO GRC3-000-PO-010

1. PROPÓSITO

La presente política tiene como finalidad desarrollar los lineamientos y directrices aplicables a recopilación, almacenamiento y gestión de Datos Personales con el objeto de garantizar adecuado tratamiento y protección.

2. AMBITO Y APLICACIÓN

La Política es aplicable a todas las empresas que forman parte de la Unidad de Negocio Perú, en adelante, indistintamente, la Empresa o la Compañía, y es de obligatorio cumplimiento a todos los Colaboradores de dichas empresas, incluyendo a sus directores, alta administración, gerentes, trabajadores en general y en lo que corresponda, cualquier tercero relacionado o vinculado a la Compañía contractual o comercialmente.

La Compañía adoptará los mecanismos pertinentes para que sus proveedores y clientes y terceros relacionados conozcan y cumplan, en lo que les corresponde con las estipulaciones de la Política.

La Política alcanza a la información física, así como la información almacenada electrónicamente y/o transmitida por correo electrónico. En ese sentido, es aplicable a los bancos de datos personales registrados o por registrarse ante la Autoridad Nacional de Protección de Datos Personales (en adelante la "Autoridad").

3. REFERENCIA Y LEGISLACIÓN ASOCIADA

La presente política se basa en el siguiente marco normativo de protección de datos personales del Perú:

- Ley N° 29733 de Protección de Datos Personales
- Decreto Supremo N° 016-2024-JUS Reglamento de la Ley N° 29733
- Directiva de Seguridad de la Información
- Guía práctica para la observancia del deber de informar
- Tratamiento de datos personales mediante sistemas de videovigilancia

Para efectos de la presente política, las normas peruanas de protección de datos personales serán denominadas en adelante "LPDP".

4. DECLARACIÓN DE LA POLÍTICA

4.1. Principios

La Empresa adopta medidas organizativas, técnicas y legales necesarias (para mayor detalle, ver **anexo 1**) para evitar, de manera razonable, algún incumplimiento de conformidad con lo establecido en el LPDP. En esa línea, a continuación, se desarrollan los principios a los cuales se compromete la Empresa respecto del cumplimiento de las disposiciones la LPDP:

4.1.1. Principio de legalidad

El tratamiento de Datos Personales se hace en estricto cumplimiento de las disposiciones establecidas en la LPDP. Se prohíbe la recopilación de los Datos Personales por medios fraudulentos, desleales o ilícitos.

4.1.2. Principio de consentimiento

El Tratamiento de Datos Personales requiere el consentimiento de su titular.

4.1.3. Principio de finalidad

Los Datos Personales deben ser recopilados para una finalidad determinada, explícita y lícita. El Tratamiento de Datos Personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación.

4.1.4. 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.

4.1.5. Principio de calidad

Los Datos Personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopilados. Los Datos Personales deben conservarse de forma tal que se garantice su seguridad y solo deben ser conservados por el tiempo necesario para cumplir con la finalidad del Tratamiento.

4.1.6. Principio de seguridad

La Empresa debe adoptar las medidas técnicas, organizativas y legales necesarias (para mayor detalle, ver **anexo 1** adjunto a la presente) para garantizar la seguridad de los Datos Personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y considerando la sensibilidad de la información.

4.1.7. 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 ARCO (Acceso, Rectificación, Cancelación y Oposición).

4.1.8. Principio de Flujo Transfronterizo y el nivel de protección adecuado en países distintos al Perú

La Empresa 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 la LPDP o por los estándares internacionales en la materia cuando realiza Flujo Transfronterizo de Datos Personales.

4.1.9. Principio de transparencia

El tratamiento de Datos Personales debe realizarse de forma clara, comprensible, accesible y permanente. La Empresa debe informar al titular del Dato Personal sobre las condiciones del tratamiento, las finalidades, los derechos que puede ejercer y cualquier cambio relevante en estos aspectos. Este principio rige tanto en entornos físicos como digitales.

4.1.10. Principio de responsabilidad proactiva

La Empresa debe implementar medidas legales, técnicas y organizativas adecuadas para asegurar y demostrar el cumplimiento del régimen de protección de Datos Personales. Este principio implica no solo cumplir con la ley, sino anticiparse a los riesgos del tratamiento mediante mecanismos preventivos como la evaluación de impacto, protocolos de seguridad, auditorías internas y formación continua.

4.1.11. Recursos asignados y cumplimiento oportuno e idóneo

La Empresa asigna los recursos suficientes para la implementación de los controles de seguridad adecuados para cada uno de los Bancos de Datos Personales, en función a la naturaleza y complejidad de sus tratamientos.

4.1.12. Adecuación continúa a la normativa de privacidad

La Empresa adecuará de manera continua y sostenible las futuras actualizaciones de la normativa de privacidad de la LPDP. Asimismo, se orientará a los responsables de Tratamiento de Datos Personales respecto del cumplimiento de las disposiciones establecidas en la LPDP.

4.1.13. Compromiso de la alta dirección y sus colaboradores

La Empresa es responsable de garantizar el cumplimiento de esta política y promover de forma razonable su mejora continua.

Los Colaboradores conocen, entienden y se comprometen a cumplir con el contenido de esta Política y demás normas internas relacionadas. Adicionalmente todo responsable del Tratamiento de Datos Personales será debidamente capacitado respecto en el contenido de esta Política, la Matriz de Datos Personales de la Empresa y el ecosistema de Datos Personales la que incluye los siguientes aspectos:

- Datos recopilados.
- Medios plataformas de recepción.
- Datos Personales Sensibles.
- Responsabilidad de los titulares de Bancos de Datos.
- Lugar de almacenamiento.
- Bancos de Datos actualmente registrados.
- Creación y recolección de datos personales.
- Gestión de solicitudes ARCO.
- Medidas de seguridad.

5. LINEAMIENTOS

Cumplimiento a la normativa y cumplimiento regulatorio

1) La Empresa protege los Datos Personales y respeta todos los principios de protección de Datos Personales señalados en la LPDP.

Sostenibilidad del programa de privacidad

2) La Empresa establece una estructura organizacional que incluye roles y responsabilidades, adecuadas a la LPDP, que le permite gobernar la protección de Datos Personales de manera sostenible en el tiempo.

Inscripción y actualización de Bancos de Datos Personales ante La Autoridad

3) La Empresa inscribe y actualiza periódicamente los Bancos de Datos Personales de su titularidad y flujos transfronterizos (de ser aplicables) en el Registro Nacional de Protección de Datos Personales (RNPDP), de acuerdo con lo señalado en la LPDP.

Recolección de Datos Personales

4) La Empresa reconoce la importancia de ejercer sus responsabilidades respecto del Tratamiento de Datos Personales en concordancia con los principios reconocidos por la normativa de protección de Datos Personales y particularmente los principios de finalidad y de proporcionalidad.

5) La Empresa tratará Datos Personales Sensibles cuando:

- El Titular haya dado su autorización explicita a dicho tratamiento, salvo en los casos que, por Ley, no sea requerido el otorgamiento de dicha autorización.
- El tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
- El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- El tratamiento tenga una finalidad histórica, estadística o científica, o dentro del marco de procesos de mejoramiento, siempre y cuando se adopten las medidas conducentes a la supresión de identidad de los titulares. Informar al Titular que por tratarse de Datos Personales Sensibles no está obligado a autorizar su tratamiento.

Se podrá hacer uso y tratamiento de los datos catalogados como Datos Personales Sensibles siempre y cuando se tenga un consentimiento previo y expreso. La empresa deberá informar al Titular lo siguiente:

- Que no está obligado a autorizar el tratamiento de sus datos sensibles.
- De forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de Dato Personal, el objeto y finalidad del tratamiento.

Elementos de decisión de creación de Bancos de Datos Personales

6) La Empresa realiza una proyección hipotética de necesidades que requieran la recopilación de Datos Personales en base a la naturaleza y alcance de sus actividades y proyectos que realice, para lo cual considera los siguientes elementos en la decisión de creación de Bancos de Datos Personales:

- Determinación de la finalidad que justifique la recolección de Datos Personales a ser recopilados, la que debe ser determinada, explícita y lícita.
    - El Tratamiento de los Datos Personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal en el momento de su recopilación.

- Determinación de qué tipos de Datos Personales se recopilarán y proyectar si es que estos serán Datos Personales Sensibles.

- Determinar la plataforma o plataformas de recolección, las cuales pueden ser físicas manejadas en papel (como contratos) o informáticas/computarizadas (como correos electrónicos, etc.).

- Obtención del consentimiento de los Titulares de Datos Personales.
    - Se realiza una evaluación sobre la pertinencia o necesidad de obtener el consentimiento expreso del Titular de Datos Personales, para ello reconoce la existencia de excepciones normativas.
    - El tratamiento de Datos Personales sólo se realizará con el consentimiento previo, libre, expreso, inequívoco e informado del Titular, salvo las excepciones legales previstas. Para Datos Personales Sensibles, el consentimiento del Titular se recabará necesariamente por escrito, mediante firma manuscrita, digital, electrónica, o cualquier modalidad admitida por el ordenamiento jurídico, conforme a lo dispuesto en los artículos 2, 5 y 8 del Reglamento de la LPDP.

- Se recopilan los Datos Personales Sensibles obteniendo el consentimiento expreso de los titulares optando entre las siguientes maneras de expresión de consentimiento: Firma manuscrita, firma digital o cualquier otro mecanismo de autenticación.

- Determinar e indicar la ubicación del Banco de Datos Personales.

- Determinar e indicar si los Datos Personales recopilados serán sometidos a Flujo Transfronterizo.
    - Se determina si los Datos Personales recopilados serán sometidos a Flujo Transfronterizo, para lo cual se obtiene el consentimiento previo, informado, expreso e inequívoco que involucre la transferencia nacional o internacional (Flujo Transfronterizo) limitándose a la finalidad que lo justifique.
    - La Empresa garantiza el nivel adecuado de seguridad del receptor de los Datos Personales transferidos y pone en conocimiento a la Dirección General de Protección de Datos Personales de conformidad con el formato previsto para ello.

Actualmente La Empresa tiene registrados los bancos de datos personales listados en el **Anexo 2 Cartillas Informativas de Banco de Datos Personales**

Deber de informar

Conforme al artículo 6 del Reglamento LPDP, cuando se recaben Datos Personales, se informará de manera clara y sencilla lo siguiente:

- Identidad y domicilio del responsable ([datos antes indicados]).
- Finalidad(es) específica(s) del tratamiento: [describir con precisión cada finalidad, evitando frases genéricas como “otros fines”].

- Identidad de los destinatarios nacionales o internacionales de los datos, de ser el caso.
- Existencia e identificación del banco de datos personales en el que serán almacenados [nombre del banco de datos y número de inscripción, si corresponde].
- Carácter obligatorio o facultativo de sus respuestas, y los datos obligatorios para cumplir con cada finalidad.
- Las consecuencias de proporcionar o no proporcionar sus datos personales.
- Si corresponde, la transferencia nacional o internacional de los datos y la finalidad de la misma.
- El plazo de conservación de los datos personales ([especificar el plazo]).
- Los mecanismos para ejercer los derechos de acceso, rectificación, cancelación, oposición y revocatoria del consentimiento, detallando el canal, procedimiento y plazos.
- Información sobre la existencia de decisiones automatizadas, incluida la elaboración de perfiles, cuando corresponda, y sus consecuencias para el titular.

La negativa a consentir el tratamiento de Datos Personales para finalidades adicionales no afectará la prestación del servicio o la relación principal.

Seguridad de la información y Ciberseguridad

7) Cuando terceros (proveedores, aliados, etc.) realicen tratamiento de Datos Personales por encargo, la Empresa suscribirá un contrato de encargo de tratamiento de Datos Personales que establecerá expresamente: El objeto, la duración, la naturaleza y finalidad del tratamiento, los tipos de datos y categorías de titulares, las obligaciones del encargado, el destino de los datos al término de la prestación, y demás exigencias previstas en el artículo 33 del Reglamento de la LPDP. El encargado debe garantizar el cumplimiento de la Ley de PDP y de suReglamento.

8) La Empresa asegura el cumplimiento razonable de las medidas y los controles de seguridad de la información y ciberseguridad señalados en la LPDP.

9) En aplicación de la Directiva de Seguridad publicada por la Autoridad, se categoriza los niveles de complejidad del Tratamiento de Datos Personales en básico, simple, intermedio, complejo y crítico en atención al cumplimiento o no de los siguientes criterios:

- Volumen de registros: número de Titulares de Datos Personales que consienten el tratamiento de sus Datos Personales (hasta 50, hasta 100, hasta 1000 e indeterminado).
- Número de Datos Personales en Banco de Datos Personales: Hasta 5 o más Bancos de Datos Personales.
- Tiempo de Tratamiento de Datos Personales: Mayor a 1 año o indeterminado.
- Localización de Bancos de Datos Personales: Si el Titular del Banco de Datos Personales es del tipo persona jurídica o entidad pública con múltiples localizaciones desde las cuales se tiene acceso al Banco de Datos Personales o realiza Tratamiento de los Datos Personales desde una sola ubicación.
- Existencia de Datos Personales Sensibles: Si el banco de datos personales incluye datos sensibles.
- El inventario de activos y bancos de Datos Personales deberá mantenerse actualizado e incluir información sobre ubicación, responsable, categoría de datos, finalidades, nivel de seguridad asignado y transferencias nacionales/internacionales asociadas.

10) En casos de tratamiento mediante servicios tecnológicos tercerizados (cloud, SaaS, hosting, etc.), La Empresa garantizará que los proveedores no asuman la titularidad de los bancos de Datos Personales, mantendrá control sobre las decisiones de tratamiento, exigirá la confidencialidad y destrucción de los datos una vez concluido el servicio, conforme al artículo 29 y siguientes del Reglamento de la LPDP.

11) En aplicación del análisis de los criterios descritos en el numeral anterior La Empresa ha determinado que la calidad de los Bancos de Datos que administra se ubica en las categorías de seguridad intermedia y compleja por lo que se aplican las siguientes recomendaciones expuestas en la Norma Técnica NTP-ISO/IEC 27001 y Directiva de Seguridad de ANPDP:

- **Gestión de los medios utilizados para el tratamiento de datos personales, almacenamiento y transporte:**
  Se considera:
  - Activos asociados con información e instalaciones de procesamiento de información deben ser identificados e inventariados.

- Los medios que contienen información deben ser protegidos contra el acceso no autorizado, el mal uso o la corrupción durante el transporte.

- **Revisión y registro de los privilegios de accesos:**
  Se consideran los siguientes elementos:
  - Control de acceso físico (en general y a datos sensibles)
  - Cuando se contengan datos sensibles, ubicar banco de datos personales en un ambiente aislado protegido por cerradura o similar mecanismo, donde la responsabilidad del mecanismo de acceso recae en el titular de banco de datos personales o un responsable delegado por el titular de banco de datos personales.
  - Control de acceso informático (en general y a datos sensibles)
  - Los usuarios deben tener un identificador único de acceso asociado a perfiles de usuarios y los accesos autorizados para cada uno de ellos. Asimismo, se debe contar con mecanismos de restricción para evitar el acceso a recursos no autorizados. La autenticación de usuarios puede estar basada en contraseñas o mecanismos de fuerte autenticación como el uso de toquen, dispositivos biométricos, firmas digitales, tarjetas inteligentes, tarjetas de coordenadas, entre otros.
  - Identificación de acceso realizados a los datos personales para tratamiento
  - Implementar un registro de accesos al banco de datos personales, el cual debe contener al menos los siguientes campos:
    1. Fecha y hora de acceso;
    2. Persona o personas que realiza el acceso;
    3. Identificador del titular de los datos personales a tratar:
    4. Motivo del acceso.
  - Asignación y retiro de privilegios
    El titular, o quien éste designe, debe asignar o retirar privilegios a los usuarios con acceso a los datos personales contenidos en el banco de datos personales. Dicha operación debe ser registrada.

- **Gestión y uso de contraseñas:**
  Se debe controlar la asignación y el uso de las contraseñas de los usuarios de los sistemas de información que realizan tratamiento de datos personales mediante la adopción de las siguientes medidas:
  a) Solicitar que se mantenga el secreto de contraseñas.
  b) Cuando se utilice un servidor de autenticación, este debe almacenar las contraseñas de manera cifrada.
  c) Permitir que el cambio de contraseña cuando el usuario lo considere necesario.

- **Conservación, respaldo y recuperación de los** Datos Personales
  En los ambientes en los que se procese, almacene o transmita la información se diseñarán e implementarán como mínimo los siguientes controles de seguridad:
  1. Controles para mantener las áreas seguras.
  2. Controles para mantener los equipos seguros dentro y fuera de las instalaciones.
  3. Controles para garantizar la generación de copias de respaldo seguras y continuas y verificación de integridad de las mismas.

- **Controles para mantener las áreas seguras**
  Los controles para mantener las áreas seguras son los siguientes:
  1. Perímetros de seguridad que protegen áreas donde se realice el tratamiento de datos personales.
  2. Controles apropiados de ingreso para asegurar que se le permita el acceso solo al personal autorizado.
  3. Sistema contra desastres naturales, ataque maliciosos o accidentes.
  4. Procedimientos para el trabajo en áreas seguras.
  5. Control de puntos de acceso, áreas de despacho, carga y otros donde personas no autorizadas pueden ingresar al local, y de ser el caso aislar las instalaciones de procesamiento de la información para evitar el acceso no autorizado.

- **Flujo transfronterizo:**
  El emisor del flujo transfronterizo debe garantizar las medidas de seguridad del receptor. Dicha aceptación debe producirse por escrito.

El titular de Banco de Datos debe asegurar el cumplimiento de lo siguiente:

- Poner en conocimiento de la Dirección General de Protección de Datos Personales, incluyendo información que se requirió para la transferencia, la finalidad y la identificación del receptor.
- Garantizar que el país destinatario de dicha información cuente con un nivel de protección adecuado o suficiente entendido como el que abarca por lo menos la consignación y el respeto de los principios rectores de la Ley.
- Para determinar el nivel adecuado de protección de datos de un país, la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales emitirá una resolución a efectos de determinar si determinado años cuanta con protección equiparable a lo dispuesto en la LPDP y y el Reglamento.
- La referida evaluación precitada considera como mínimo y de modo concurrente, los siguientes criterios:
    - La existencia de un marco jurídico legal de protección de datos personales.
    - La existencia de principios para el tratamiento de los datos personales.
    - La existencia de normas que reconozcan y garanticen los derechos de los titulares de datos y que puedan disponer de vías para ejercer los mismos.
    - La existencia de una autoridad encargada de la protección de datos personales, o aquellas que hagan sus veces, para supervisar y sancionar por infracciones a la normativa, cuando corresponda.
- La resolución a la que referidas líneas arriba se emite de oficio, a solicitud de parte o como consecuencia de las normas sectoriales que compelen a los sectores a recabar opinión técnica de la Autoridad Nacional de Protección de Datos Personales.

Lo indicado no se aplica en los siguientes casos:

1. Acuerdos en el marco de tratados internacionales sobre la materia en los cuales la República del Perú sea parte.
2. Cooperación judicial internacional.
3. Cooperación internacional entre organismos de inteligencia para la lucha contra el terrorismo, tráfico ilícito de drogas, lavado de activos, corrupción, trata de personas y otras formas de criminalidad organizada.
4. Cuando los Datos Personales sean necesarios para la ejecución de una relación contractual en la que el titular de Datos Personales sea parte.
5. Cuando se trate de transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme a la ley aplicable.
6. Cuando el titular de los Datos Personales haya dado su consentimiento previo, informado, expreso e inequívoco.

Uso de cámaras de videoseguridad

12) La Empresa utiliza cámaras de videoseguridad en concordancia con las disposiciones de la normativa de protección de Datos Personales para los siguientes propósitos:

- Control laboral
  El control laboral se justifica en el poder de dirección del empleador, sólo se realiza cuando sea pertinente, adecuado y no excesivo para el cumplimiento de tal fin.
  La finalidad de la grabación de video seguridad es el control y la supervisión de la prestación laboral.
  No es necesaria la obtención de consentimiento, no obstante, sí precisa del cumplimiento del deber de informar.
  La grabación solo será de imágenes. Excepcionalmente de audio cuando sean relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivadas de la actividad que se desarrolle en el centro de trabajo.
  La grabación se restringe a espacios indispensables para satisfacer las finalidades del control laboral. No se admite su instalación en zonas de descanso o esparcimiento de trabajadores (vestuarios, servicios higiénicos, comedores o análogos).

- Vigilancia y seguridad
  La pertinencia de la utilización de cámaras de videovigilancia usadas con terceros no relacionados con la empresa se justifica en la finalidad de vigilancia y seguridad en concordancia con el principio de proporcionalidad.

La grabación solo será de imágenes. Excepcionalmente de audio cuando se pondere la necesidad de controlar riesgos de seguridad en las instalaciones, bienes y personas en zonas de acceso compartido con Colaboradores. No es necesario la obtención de consentimiento, no obstante, sí precisa del cumplimiento del deber de informar.

- Texto para uso de cámaras de videovigilancia
  Se usará el texto propuesto en la Directiva de Tratamiento de los Datos Personales mediante Sistemas de Videovigilancia y será presentado en medios informáticos, digitalizados o impresos **(Ver GRC1-000-TA-008 Cartilla Informativa Videovigilancia).**

- Cumplimiento del deber de información
  Se garantiza mantener informado a los Titulares de Datos Personales obtenidos a través de cámaras de videovigilancia mediante el uso de carteles informativos de acuerdo con lo dispuesto en la LPDP **(Ver modelo del cartel informativo en el anexo 3).**

- Del plazo para el almacenamiento de la información grabada
  Será de treinta (30) días y hasta un máximo sesenta (60) días hábiles. Trascurrido dicho plazo, la información grabada se elimina definitivamente de conformidad con lo establecido en la LPDP.

- Transferencia de datos personales recopilados mediante cámaras de videovigilancia
  La Empresa cumplirá con su deber de colaboración en la transferencia de Datos Personales captados por los sistemas de videovigilancia de acuerdo con la LPDP y, en particular, en los siguientes casos:
  - Lo recopilado sea requerido por orden judicial o por una entidad pública en cumplimiento de sus funciones.
  - Cuando lo recopilado deba ser puesto a disposición o sea requerido por la Policía Nacional del Perú o por el Ministerio Público, en el ejercicio de sus funciones, en supuestos necesarios para la prevención, investigación, detección o represión de infracciones penales o delitos, y siempre que estas peticiones se den motivadamente y el tratamiento de estas respondan a la finalidad del requerimiento realizado.

Incidentes de Seguridad

13) En caso de un incidente de seguridad de Datos Personales que genere exposición de grandes volúmenes de los mismos, en cantidad o tipo de datos, o que pueda afectar a un gran número de personas o cuando se trate de datos sensibles o cuando se produzca un perjuicio evidente a otros derechos o libertades del titular del dato personal, el titular del banco de datos o el responsable del tratamiento debe notificar a la Autoridad Nacional de Protección de Datos Personales como máximo dentro de las cuarenta y ocho (48) horas posteriores a haber tomado conocimiento del incidente. Si dicha notificación se efectúa en un tiempo superior a cuarenta y ocho (48), debe ir acompañada de la indicación de los motivos y/o sustento probatorio de tal dilación. Esta obligación permanece aun cuando el responsable de tratamiento de Datos Personales considere que tal incidente haya sido subsanado o resuelto internamente.

14) La Empresa notificará el incidente a la Autoridad Nacional de Protección de Datos Personales dentro de los plazos establecidos en la normativa vigente, incluyendo al menos:

- La naturaleza del incidente de seguridad de los Datos Personales, inclusive, cuando sea posible, los tipos de datos y el número aproximado de titulares de datos afectados.
- El nombre y los datos de contacto del Oficial de Datos Personales o de otro punto de contacto en el que pueda obtenerse más información.
- Las posibles consecuencias del incidente de seguridad de los Datos Personales.
- Las medidas adoptadas o propuestas por el titular del banco de datos o responsable del tratamiento para poner remedio a la violación de la seguridad de los Datos Personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos

15) Si la Empresa advierta un incidente de seguridad de Datos Personales que afecte al Titular de los mismos en otros de sus derechos, debe comunicarlo dentro de las cuarenta y ocho (48)a dicho titular sin dilación indebida, en un lenguaje sencillo y claro para su comprensión, así como de las medidas adoptadas para mitigar sus efectos. Si dicha comunicación se efectúa en un tiempo superior a las cuarenta y ocho (48) debe ir acompañada de la indicación de los motivos de tal dilación.

16) Cuando el incidente de seguridad de Datos Personales no produjo la afectación antes descrita y fue superado totalmente por las medidas adoptadas no subsiste la obligación de comunicar dicho incidente al Titular de los datos personales.

17) En caso que el incidente de seguridad de Datos Personales se desarrolle en y/o mediante el entorno digital la notificación se realiza, además de la Autoridad Nacional de Protección de Datos Personales, al Centro Nacional de Seguridad Digital para su incorporación al Registro Nacional de Incidentes de Seguridad Digital conforme a lo establecido en el Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, su Reglamento y normas complementarias.

18) La Empresa debe documentar cualquier incidente de seguridad, incluyendo los hechos relacionados a ello, sus efectos y las medidas adoptadas. Dicha documentación permite a la Autoridad Nacional de Protección de Datos Personales verificar el cumplimiento de las obligaciones referidas a esta materia.

Gestión de solicitudes de Derechos ARCO

19) La Empresa pone a disposición un sistema, plataforma o correo electrónico que consolide la recepción de las solicitudes de ejercicio de Derechos ARCO de acuerdo con lo reconocido en la LPDP. Las solicitudes de Derechos ARCO se describen a continuación:

- Derecho de acceso: Solicitud dirigida a obtener información sobre sus Datos Personales objeto de tratamiento, así como, la forma en que fueron recopilados, razones que motivaron la recopilación y las transferencias a las que fueron sometidos o las que se prevén realizar.

Consideraciones respecto del derecho de acceso:

Subsanación: En caso que la solicitud no cumpla con los requisitos del artículo 63 del Reglamento de la LPDP. La Empresa, en un plazo de cinco (5) días, contado desde el día siguiente de la recepción de la solicitud, formula las observaciones que no puedan ser salvadas de oficio, invitando al titular a subsanarlas dentro de un plazo máximo de cinco (5) días. Transcurrido el plazo señalado sin que ocurra la subsanación se tiene por no presentada la solicitud.

En el caso que la información proporcionada en la solicitud sea insuficiente o errónea de forma que no permita su atención, La empresa, cuando corresponda, puede requerir dentro de los siete (7) días siguientes de recibida la solicitud, información o documentación adicional al titular de los datos personales para atenderla.

En un plazo de diez (10) días de recibido el requerimiento, contado desde el día siguiente de la recepción del mismo, el titular de datos personales debe acompañar la documentación adicional que estime pertinente para fundamentar su solicitud. En caso contrario, se tiene por no presentada dicha solicitud.

Plazo de respuesta: Veinte (20) días hábiles desde el día siguiente de la fecha de recepción de la solicitud o desde la fecha de recepción de la solicitud subsanada.

Extensiones: La respuesta extendiendo el plazo para atender a la solicitud debe comunicarse al solicitante dentro del plazo fijado para su respuesta, justificando los motivos de la extensión. El plazo para atender la solicitud puede ser de máximo veinte (20) días hábiles adicionales al plazo inicial.

Medios para el cumplimiento del derecho de acceso: La información correspondiente al derecho de acceso, a opción del titular de los Datos Personales, puede suministrarse por escrito, por medios electrónicos, telefónicos, de imagen u otro idóneo para tal fin.
El Titular de los Datos Personales puede optar por alguna de las siguientes formas:

- Visualización en sitio.
- Escrito, copia, fotocopia o facsímil.
- Transmisión electrónica de la respuesta, siempre que esté garantizada la identidad del interesado y la seguridad y recepción de la información.

- Cualquier otra forma o medio que sea adecuado a la configuración o implantación material del banco de datos personales o a la naturaleza del tratamiento, establecido por el titular del banco de datos personales o responsable del tratamiento.

Responsabilidad de respuesta en primera instancia: Oficial de Datos Personales.

Autoridad en impugnación o falta de respuesta: Dirección General de Protección de Datos Personales.

- Derecho de rectificación: Solicitud para obtener la actualización, rectificación y/o inclusión de Datos Personales contenidos en los Bancos de Datos Personales que precise:
  a) Por la actualización se modifica los Datos Personales que hayan cambiado a la fecha de la solicitud.
  b) Por la rectificación se corrigen los Datos Personales contenidos en Bancos de Datos Personales que sean erróneos, inexactos o falsos.
  c) Por la inclusión se incorporan/modifican los Datos Personales contenidos en Bancos de Datos Personales con la información nueva proporcionada por el Titular de Datos Personales que presenta la solicitud.

Consideraciones respecto del derecho de rectificación:

Subsanación: En caso que la solicitud no cumpla con los requisitos del artículo 63 del Reglamento de la LPDP. La Empresa, en un plazo de cinco (5) días, contado desde el día siguiente de la recepción de la solicitud, formula las observaciones que no puedan ser salvadas de oficio, invitando al titular a subsanarlas dentro de un plazo máximo de cinco (5) días. Transcurrido el plazo señalado sin que ocurra la subsanación se tiene por no presentada la solicitud.

En el caso que la información proporcionada en la solicitud sea insuficiente o errónea de forma que no permita su atención, La empresa, cuando corresponda, puede requerir dentro de los siete (7) días siguientes de recibida la solicitud, información o documentación adicional al titular de los datos personales para atenderla.

En un plazo de diez (10) días de recibido el requerimiento, contado desde el día siguiente de la recepción del mismo, el titular de datos personales debe acompañar la documentación adicional que estime pertinente para fundamentar su solicitud. En caso contrario, se tiene por no presentada dicha solicitud.

Plazo de respuesta: Diez (10) días hábiles desde el día siguiente de la fecha de recepción de la solicitud o desde la fecha de recepción de la solicitud subsanada.

Extensiones: La respuesta extendiendo el plazo para atender a la solicitud debe comunicarse al solicitante dentro del plazo fijado para su respuesta. El plazo para atender la solicitud puede ser de máximo diez (10) días hábiles computados desde el desde el día siguiente a la fecha de la comunicación de extensión del plazo para atender a la solicitud, siempre y cuando las circunstancias lo justifiquen.

Responsabilidad de respuesta en primera instancia: Oficial de Protección de Datos.

Autoridad en impugnación o falta de respuesta: Dirección General de Protección de Datos Personales.

- Derecho de cancelación y supresión: Solicitud para obtener la cancelación o supresión de Datos Personales de Bancos de Datos Personales que hayan dejado de ser necesarios en función de su finalidad, finalizado el plazo de su tratamiento o haya revocado su consentimiento. La solicitud de supresión o cancelación puede referirse a todos los Datos Personales del Titular contenidos en un banco de datos personales o solo a alguna parte de ellos.

  La Empresa debe documentar ante el Titular de los Datos Personales haber cumplido con lo solicitado e indicar las transferencias de los datos suprimidos, identificando a quién o a quiénes fueron transferidos, así como la comunicación de la supresión correspondiente.

La supresión no procede cuando los datos personales deban ser conservados en virtud de razones históricas, estadísticas o científicas de acuerdo con la legislación aplicable o, en su caso, en las relaciones contractuales entre el responsable y el Titular de los Datos Personales, que justifiquen el tratamiento de los mismos.

Consideraciones respecto del derecho de cancelación:

Subsanación: En caso que la solicitud no cumpla con los requisitos del artículo 63 del Reglamento de la LPDP. La Empresa, en un plazo de cinco (5) días, contado desde el día siguiente de la recepción de la solicitud, formula las observaciones que no puedan ser salvadas de oficio, invitando al titular a subsanarlas dentro de un plazo máximo de cinco (5) días. Transcurrido el plazo señalado sin que ocurra la subsanación se tiene por no presentada la solicitud.

En el caso que la información proporcionada en la solicitud sea insuficiente o errónea de forma que no permita su atención, La empresa, cuando corresponda, puede requerir dentro de los siete (7) días siguientes de recibida la solicitud, información o documentación adicional al titular de los datos personales para atenderla.

En un plazo de diez (10) días de recibido el requerimiento, contado desde el día siguiente de la recepción del mismo, el titular de datos personales debe acompañar la documentación adicional que estime pertinente para fundamentar su solicitud. En caso contrario, se tiene por no presentada dicha solicitud.

Plazo de respuesta: Diez (10) días hábiles desde el día siguiente de la fecha de recepción de la solicitud o desde la fecha de recepción de la solicitud subsanada.
Extensiones: La respuesta extendiendo el plazo para atender a la solicitud debe comunicarse al solicitante dentro del plazo fijado para su respuesta. El plazo para atender la solicitud puede ser de máximo diez (10) días hábiles computados desde el desde el día siguiente a la fecha de la comunicación de extensión del plazo para atender a la solicitud, siempre y cuando las circunstancias lo justifiquen.

Responsabilidad de respuesta en primera instancia: Oficial de Protección de Datos.

Autoridad en impugnación o falta de respuesta: Dirección General de Protección de Datos Personales.

- Derecho de oposición: El Titular de Datos Personales tiene derecho a oponerse en cualquier momento, a efectos de que no se lleve a cabo el tratamiento de sus datos personales o se cese en el mismo, cuando no hubiere prestado su consentimiento para su recopilación por haber sido tomados de fuente de acceso al público.

  Aun cuando hubiera prestado consentimiento, el Titular de Datos Personales tiene derecho a oponerse al tratamiento de sus Datos Personales, si acredita la existencia de motivos fundados y legítimos relativos a una concreta situación personal que justifiquen el ejercicio de este derecho.

  En caso que la oposición resulte justificada el Titular del banco de Datos Personales o responsable de tratamiento debe proceder al cese del tratamiento que ha dado lugar a la oposición.

  Salvo que exista relación contractual previa que sustente dicho tratamiento, cuando los Datos Personales son tratados para fines de publicidad y prospección comercial, incluido la elaboración de perfiles, el Titular de Datos Personales puede ejercer su derecho de oposición, en cualquier momento, de acuerdo con los requisitos del Reglamento de la LPDP.

  Cuando los Datos Personales son tratados en internet, el ejercicio de derecho de oposición puede incluir la desindexación de los Datos Personales.

Consideraciones respecto del derecho de oposición:

Subsanación: En caso que la solicitud no cumpla con los requisitos del artículo 63 del Reglamento de la LPDP,a Empresa, en un plazo de cinco (5) días, contado desde el día siguiente de la recepción de la solicitud, formula las observaciones que no puedan ser salvadas de oficio, invitando al titular a subsanarlas dentro de un plazo máximo de cinco (5) días. Transcurrido el plazo señalado sin que ocurra la subsanación se tiene por no presentada la solicitud.

En el caso que la información proporcionada en la solicitud sea insuficiente o errónea de forma que no permita su atenció. la Empresa, cuando corresponda, puede requerir dentro de los siete (7) días siguientes de recibida la solicitud, información o documentación adicional al Titular de los Datos Personales para atenderla.

En un plazo de diez (10) días de recibido el requerimiento, contado desde el día siguiente de la recepción del mismo, el titular de Datos Personales debe acompañar la documentación adicional que estime pertinente para fundamentar su solicitud. Caso contrario, se tiene por no presentada dicha solicitud.

Plazo de respuesta: Diez (10) días hábiles desde el día siguiente de la fecha de recepción de la solicitud o desde la fecha de recepción de la solicitud subsanada.

Extensiones: La respuesta extendiendo el plazo para atender a la solicitud debe comunicarse al solicitante dentro del plazo fijado para su respuesta. El plazo para atender la solicitud puede ser de máximo diez (10) días hábiles computados desde el desde el día siguiente a la fecha de la comunicación de extensión del plazo para atender a la solicitud, siempre y cuando las circunstancias lo justifiquen.

Responsabilidad de respuesta en primera instancia: Oficial de Protección de Datos.

Autoridad en impugnación o falta de respuesta: Dirección General de Protección de Datos Personales.

20) La Empresa informa a los solicitantes de cualquiera de las acciones listadas anteriormente que ante el supuesto de denegatoria de su solicitud les asiste el derecho de recurrir ante la DGPDP en vía de reclamación.

21) Como manifestación del derecho de acceso, el Titular puede solicitar los Datos Personales sobre sí mismo, que haya facilitado a un responsable o titular de banco de datos, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable o titular de banco de datos personales cuando:

- El tratamiento esté basado en el consentimiento o en una relación contractual en la que el Titular es parte; o,
- El tratamiento se ejerza mediante medios automatizados.

Al ejercer la portabilidad, el Titular tiene derecho a que sus Datos Personales se transmitan directamente de un responsable o titular del banco de datos a otro cuando sea técnicamente posible lo que no incluye su ejercicio imponga una carga financiera excesiva, técnica excesiva o irrazonable al responsable o encargado del tratamiento.

En caso que la Empresa no cuente con la posibilidad técnica referida debe acreditar tal situación ante un eventual requerimiento de la Autoridad Nacional de Protección de Datos Personales en el marco de un procedimiento trilateral de tutela, cuando así corresponda.

6. RESPONSABILIDADES

La Empresa define las responsabilidades de los involucrados en el tratamiento de datos personales de acuerdo con los siguientes roles:

6.1. Responsable de tratamiento de datos personales

Colaborador designado como responsable de un Banco de Datos Personales que tiene la función gestión de un Banco de Datos, así como verificar el cumplimiento de las medidas de seguridad y demás lineamientos establecidos en esta Política.

Responsabilidades:

- Supervisar y gestionar los Bancos de Datos Personales existentes (inscritos o no).
- Supervisar y controlar el acceso de otros Colaboradores autorizados para acceder al contenido de los Bancos de Datos Personales.
- Reportar al Oficial de Datos Personales cualquier incidente, o sospecha de incidente que considere afecte o pudiera afectar Datos Personales o la privacidad de alguna persona física.
- Informar a los demás Colaboradores del área al que pertenezca sobre cambios que se produzcan en los lineamientos de la presente política.
- Recopilar consultas sobre el Tratamiento de Datos Personales de otros Colaboradores del área al que pertenezca.

6.2. Oficial de Cumplimiento / Oficial de Protección de Datos

El Oficial de Cumplimiento de la Empresa ejerce la función de Oficial de Protección de Datos de la Empresa.

Este rol debe cumplir con las siguientes características:

- Autonomía y jerarquía en la compañía.
- Conocimiento razonable de los procesos de negocio y flujos de Datos Personales en la Empresa.
- Cualidades profesionales y, en particular, conocimientos especializados y práctica en materia de protección de Datos Personales debidamente acreditados, que le permitan desempeñar sus funciones de manera eficiente.
- No ocupar cargos de decisión sobre los fines y medios del tratamiento.
- Acceso a los recursos necesarios para el ejercicio de sus funciones.

Asimismo, administra la presente Política y es responsable de:

- Actualizar anualmente (en caso aplique) el contenido de la presente política o ante algún cambio significativo que pueda tener alguna afectación directa con la presente política.
- Difundir la presente Política, así como proveer la capacitación y concientización adecuada para su cumplimiento
- Canalizar y aclarar cualquier duda o comentario de la Política.
- Informar a la Alta Dirección sobre los avances, requerimientos, hitos, necesidades, o riesgos asociados al programa de privacidad de la Empresa.
- Comunicar y difundir las actualizaciones, cambios, excepciones y cualquier otro asunto relacionado con la materia de protección de Datos Personales y privacidad.
- Brindar orientación específica sobre cada situación o caso que se presente en aplicación a la presente política, así como atender consultas sobre lineamientos, políticas, procedimientos, manuales, talleres, o toda información documentada relacionada con protección de Datos Personales y privacidad en la Empresa.
- Liderar las medidas organizativas para el cumplimiento de a LPDP, así como coordinar y supervisa los avances realizados por los responsables de las medidas legales y técnicas en la organización.
- Asesoramiento y Verificación del Cumplimiento: Informar y asesorar al titular del banco de datos, al responsable y a los empleados sobre sus obligaciones legales. A su vez, verificar e informar sobre el cumplimiento de la Ley, el Reglamento y las políticas internas, incluyendo la correcta asignación de responsabilidades, la sensibilización del personal y las auditorías correspondientes.
- Gestión de Riesgos y Evaluaciones de Impacto (PIA/DPIA): Asesorar sobre la realización de la Evaluación de Impacto relativa a la Protección de Datos Personales cuando sea previsible un alto riesgo para los derechos y libertades, especialmente en tratamientos de datos sensibles o a gran escala.

- Cooperación y Punto de Contacto con la Autoridad: Actuar como punto de contacto y cooperar con la Autoridad Nacional de Protección de Datos Personales para todas las cuestiones relativas al tratamiento de datos.
- Realizar y documentar la comunicación formal de su designación y datos de contacto a la Autoridad Nacional de Protección de Datos Personales, así como cualquier actualización, dentro del plazo de 15 días desde su nombramiento.
- Coordinar la atención oportuna a las solicitudes de los titulares para el ejercicio de sus derechos (ARCO) y el derecho al tratamiento objetivo de sus datos.
- Ser informado oportunamente de todo incidente de seguridad para asistir y coordinar la respuesta, incluyendo la notificación a la Autoridad Nacional y a los titulares afectados cuando corresponda, conforme a los plazos y requisitos de ley.
- Planificar y ejecutar capacitaciones periódicas para promover una cultura de protección de datos en toda la organización.
- Mantener el registro de actividades de tratamiento

6.3. Colaboradores

- Conocer y cumplir las disposiciones de la presente Política.
- Solicitar orientación al Oficial de Datos Personales directamente o a través de su supervisor directo o del responsable de protección de Datos Personales designado a su área de ser el caso.
- Reportar sus inquietudes y preocupaciones al Oficial de Datos Personales respecto de la presente política directamente o a través de su supervisor directo o del responsable de protección de Datos Personales sobre los datos designados a su área de ser el caso.
- Participar en eventos o actividades promovidas localmente en cumplimiento de la LPDP y realizar las capacitaciones y certificaciones que le sean asignadas.
- Reportar al responsable de Protección de Datos Personales o al Oficial de Datos Personales cualquier incidente, o sospecha de incidente que considere afecte o pudiera afectar Datos Personales o la privacidad de alguna persona física.

6.4. Gerentes Supervisores

- Sensibilizar a los Colaboradores sobre el contenido y cumplimiento de la presente Política.
- Atender los requerimientos del Oficial de Datos Personales respecto del cumplimiento de la LPDP que dependa de su gerencia o supervisión correspondiente.
- Coordinar con el Oficial de Datos Personales y solicitar su orientación para establecer procesos y prácticas que aseguren el cumplimiento de requisitos / exigencias de la presente política.

6.5. Responsable de la Seguridad de la Información / TI

El Gerente de TI es el responsable de la Seguridad de la Información en la Empresa.

- Atender las consultas de tecnología, seguridad de la información y ciberseguridad relacionadas a Protección de Datos personales y privacidad desde el punto de vista de TI.
- Liderar las medidas técnicas para el cumplimiento de la LPDP, así como coordinar los avances realizados por los responsables de las medidas legales y organizativas.
- Cumplir con todo requerimiento del Oficial de Datos Personales respecto a los controles de seguridad de la información y ciberseguridad relacionados a la LPDP.
- Informar al Oficial de Datos Personales sobre los avances de las medidas técnicas implementadas para el cumplimiento de la LPDP.
- Coordinar y articular las actividades / avances realizados por el responsable de seguridad física en relación con el cumplimiento de la LPDP.
- Implementar las plataformas o mecanismos de consolidación de las solicitudes de Derechos ARCO poniendo a disposición una plataforma web o correo institucional.
- Establecer niveles de acceso para la modificación de Bancos de Datos y para su acceso, el cual preferiblemente debe ejecutarse en modo lectura.
- Promover que los archivos extraídos de plataformas de administración de Datos Personales sean utilizados exclusivamente para el propósito que motivó su extracción y sean posteriormente suprimidos.

6.6. Área de Seguridad Física

El Gerente de Seguridad Física es el responsable de la Seguridad Física en la Empresa

- Informar al responsable de Seguridad de la Información y al Oficial de Datos Personales sobre los avances de las medidas técnicas implementadas relacionadas a seguridad física para el cumplimiento de la LPDP en la Empresa.
- Reportar al responsable de Seguridad de la Información y al Oficial de Datos Personales sobre cualquier incidente o sospecha de incidente identificado en las revisiones periódicas en las instalaciones de la Empresa relacionadas a exposición de datos personales.
- Atender los requerimientos del responsable de Seguridad de la Información y de Oficial de Datos Personales respecto de los controles de seguridad física relacionados a la LPDP señalados en el **anexo 1**.

6.7. Área Legal

- Atender a las consultas legales relacionadas a la protección de Datos Personales y privacidad.
- Atender los requerimientos del responsable Oficial de Datos Personales respecto de los controles relacionados a las medidas legales de la LPDP descritas en el **anexo 1**.

- Liderar las medidas legales para el cumplimiento de la LPDP, así como coordinar los avances realizados por los responsables de las medidas técnicas y organizativas.
- Informar periódicamente al Oficial de Datos Personales sobre los avances de las medidas legales implementadas para el cumplimiento de la LPDP en la Empresa.

7. CONTROL Y CUMPLIMIENTO

7.1. Control y Cumplimiento

El cumplimiento de esta política es obligatorio. Todo personal deberá entender su rol y responsabilidad en relación con este Política.

7.2. Consecuencias de Incumplimiento

Desvíos e incumplimiento del presente procedimiento puede acarrear la imposición de medidas disciplinarias, que, de aplicarse, servirán como elemento correctivo y formador de nuestra cultura organizacional.

Las medidas disciplinarias deben ser justas, razonables y proporcionales a la falta cometida, respetando el marco legal correspondiente y las normas internas de la empresa.

7.3. Excepciones

Cualquier excepción a esta política deberá tratarse de manera particular y deberá estar debidamente sustentada por el solicitante y aprobada por el CEO y el Oficial de Cumplimiento.

8. ANEXOS

8.1. Anexo 1: Medidas organizativas, técnicas y legales

MEDIDAS ORGANIZATIVAS

a) Modelo de operación de privacidad (dirección, gestión, estructura organizacional, evaluación y tratamiento de riesgos de privacidad).
b) Programa de información (políticas de privacidad y tratamiento adecuado de datos personales).
c) Programa de capacitación en protección de datos personales y privacidad.

MEDIDAS TÉCNICAS

a) Seguridad de la información y Ciberseguridad (Evaluación y tratamiento de riesgos de seguridad de la información, gestión de accesos lógicos seguros, gestión de respaldos y restauraciones, antimalware, transferencia electrónica segura, monitoreo y correlación de eventos de seguridad, gestión de incidentes de ciberseguridad).
b) Seguridad Física (Almacenamiento, traslado y eliminación de información de datos personales impresos o en medios físicos).
c) Videovigilancia.

MEDIDAS LEGALES

a) Registro y/o actualización de bancos de datos personales requeridos por la LPDP.
b) Declaración del Flujo Transfronterizo ante la ANPDP.
c) Derechos ARCO (atención oportuna de las solicitudes).
d) Obtención del consentimiento.
e) Gestión de terceros / proveedores en términos de protección de datos personales y privacidad.

8.2. Anexo 2: Cartillas Informativas de Banco de Datos Personales

GRC1-000-TA-001 Cartilla Informativa Canal Ético
GRC1-000-TA-002 Cartilla Informativa Cumplimiento
GRC1-000-TA-003 Cartilla Informativa Directores
GRC1-000-TA-004 Cartilla Informativa Postulantes
GRC1-000-TA-005 Cartilla Informativa Proveedores
GRC1-000-TA-006 Cartilla Informativa Relaciones Comunitarias
GRC1-000-TA-007 Cartilla Informativa Trabajadores
GRC1-000-TA-008 Cartilla Informativa Videovigilancia
GRC1-000-TA-009 Cartilla Informativa Visitantes
GRC1-000-TA-010 Cartilla Informativa Comercial

8.3. Anexo 3: Cartel Informativo de Cámaras de videoviligancia

LEY DE PROTECCIÓN DE DATOS PERSONALES – LEY 29733

La captura de imágenes se realiza para fines de monitoreo, seguridad y de prevención de riesgos de todos nuestros visitantes y trabajadores. Los datos personales captados se almacenan en el Banco de Datos "Videovigilancia," registrado por KALLPA GENERACION S.A., con RUC N° 20538810682, con Código RNPDP-PJP N.° 28394. Para mayor información de nuestra política de privacidad visite www.kallpageneracion.com.pe/gobernanza
Puede ejercer su derecho de acceso, rectificación, cancelación y oposición, a través del correo electrónico: arco@kg.com.pe y/o en Las Calle Palmeras Nro. 435 Int. 701, San Isidro, Lima.

9. DEFINICIONES

TÉRMINO	DEFINICIÓN
Unidad de Negocio Perú	Son las compañías operativas del grupo ubicadas en el Perú. A la fecha forman parte de la Unidad de negoció Perú, Kallpa Generación S.A., Orazul Energy Perú S.A. y Kondu S.A.C.
Colaborador	Se refiere a directores, gerentes, funcionarios o empleados permanentes o temporales y practicantes o pasantes que forman parte de la Compañía.
ANPDP, La Autoridad	Autoridad Nacional de Protección de Datos Personales
Bancos de Datos Personales	Es el conjunto de datos de personas naturales computarizado o no, y estructurado conforme a criterios específicos, que permita acceder sin esfuerzos desproporcionados a los datos personales, ya sea aquel centralizado, descentralizado o repartido de forma funcional o geográfica.
Colaborador(es)	Se refiere a directores, gerentes, funcionarios o empleados permanentes o temporales y practicantes o pasantes que forman parte de la Empresa.
Dato(s) Personal(es)	Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, de localización, identificadores en línea o de cualquier otro tipo concerniente a aspectos físicos, económicos, culturales o sociales de las personas naturales que las identifica o las hace identificables. Se considera identificable cuando se puede verificar la identidad de la persona de manera directa o indirectamente a partir de la combinación de datos a través de medios que puedan ser razonablemente utilizados.. También conocida como “Información personal”.
Datos Personales Sensibles	Es aquella información relativa a datos genéticos o biométricos de la persona natural, datos neuronales, datos morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la afiliación sindical, salud física o mental u otras análogas que afecten su intimidad.
Derechos ARCO	Los Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) son derechos que tienen los Titulares de Datos Personales frente a la Empresa.
Días	Días hábiles.
Desindexación:	Es el proceso mediante el cual una dirección URL o contenido específico de un sitio web es eliminado o excluido de los resultados de motores de búsqueda. Este procedimiento, dependiendo de la situación y las circunstancias específicas, puede ser efectuado por el propietario del sitio web o por el motor de búsqueda.
Flujo Transfronterizo	Transferencia internacional de Datos Personales a un destinatario situado en un país distinto al país de origen de los Datos Personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectúe la transferencia ni el tratamiento que reciban.
Incidente de seguridad de datos personales	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.
Oficial de de Datos Personales	Profesional denominado “Oficial de Datos Personales” de la Empresa. Tiene a su cargo todas las cuestiones relativas a la protección de Datos Personales y la privacidad en las compañías de la Unidad de Negocio Perú, la verificación, asesoramiento e implementación del cumplimiento del régimen jurídico sobre protección de datos personales.
Responsable de Tratamiento de Datos Personales	Colaborador designado en cada área de la Empresa quien tiene la responsabilidad de gestionar Bases de Datos personales, así como garantizar el cumplimiento de los lineamientos establecidos en la presente política.
RNPDP	Registro Nacional de Protección de Datos Personales
Titular(es)	La persona física (natural) a quien corresponden los Datos Personales.
Tratamiento	Cualquier operación o conjunto de operaciones realizadas sobre Datos Personales o conjuntos de Datos Personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

10. CONTROL DE CAMBIOS

Versión	Fecha	Descripción	Elaborado por:	Revisado por:	Aprobado / Área - Proceso	Gerencia General	Directorio
01	Junio 2022	Documento Inicial	Consultor Externo	María Vera Nicolas Velasquez Anamaria Chalco	María Vera		Aprobado
02	Junio 2023	Actualización y ampliación de contenido, inclusión de definiciones y anexos.	Maria Vera y Nicolas Velázquez	María Vera	María Vera	Revisado Rosa María Flores-Araoz	Aprobado
03	Agosto 2025	Actualización Reglamento. Cambio codificación y nuevo formato	Interacción de Legal, TI y Cumplimiento	Maria Vera	Maria Vera	Aprobado Rosa María Flores-Araoz	-