POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

N° KALL-GRC-018

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. ALCANCE

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
- 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. DEFINICIONES

TÉRMINO	DEFINICIÓN
ANPDP, La Autoridad	Autoridad Nacional de Protección de Datos Personales
Bancos de Datos Personales	Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.

PROTECCIÓN DE DATOS PERSONALES

TÉRMINO	DEFINICIÓN
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)	Cualquier información concerniente a una persona física (natural) identificada o identificable. También conocida como "Información personal". Para mayor detalle y ejemplos ver anexo 1.
Datos Personales Sensibles	Aquellos Datos Personales que afecten a la esfera más íntima de su titular o cuya utilización indebida pueda originar discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual. Para mayor detalle y ejemplos ver anexo 1.
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.
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 / Vulneración	Es aquel que involucra incidentes o incumplimientos de privacidad y protección de Datos Personales; cualquier evento que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales; y/o cualquier tratamiento de Datos Personales de forma distinta a la finalidad por la que fueron inicialmente recabados o la comunicación, transmisión o divulgación, acceso no autorizado a dichos Datos Personales.
Oficial de Privacidad	Profesional denominado "Oficial de Privacidad" 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.
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) de Datos Personales	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.
Unidad de Negocio Perú o BU Perú.	Son las compañías operativas que a la fecha forman parte de la BU Peru Kallpa Generación S.A., Orazul Energy Perú S.A.y Kondu S.A.C.

5. DESCRIPCIÓN DE LA POLÍTICA

5.1. PRINCIPIOS

La Empresa adopta medidas organizativas, técnicas y legales necesarias (para mayor detalle, ver anexo 2) 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:

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.

2) **Principio de consentimiento**
   El Tratamiento de Datos Personales requiere el consentimiento de su titular.

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) **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.

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.

6) **Principio de seguridad**
   La Empresa debe adoptar las medidas técnicas, organizativas y legales necesarias (para mayor detalle, ver anexo 2 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.

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).

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.

9) 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.

10) 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.

11) 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 capacitados 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 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.

6. 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.

Asimismo, maneja un Procedimiento de Recolección de Datos Personales (adjunto como anexo 5).

Elementos de decisión de creación de Bancos de Datos Personales

5) 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.

- 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.

Seguridad de la información y Ciberseguridad

6) La Empresa asegura el cumplimiento razonable de las medidas y los controles de seguridad de la información y ciberseguridad señalados en la LPDP (incluyendo la Directiva de Seguridad publicada por la Autoridad). Para mayor detalle, ver anexo 2.

7) 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.

8) 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 ubican 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.

- 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.

  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

9) 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 (Hoja informativa sobre el tratamiento de datos personales - ver anexo 3).

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 4).

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.

Gestión de solicitudes de Derechos ARCO

10) 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 sí mismo almacenada en los Bancos de Datos Personales que precise, así como, la forma en que fueron recopilados, razones y las transferencias a las que fueron sometidos o las que se prevén realizar.

Consideraciones respecto del derecho de acceso:

Subsanación: Si la información es insuficiente o errónea de forma que no permita su atención, se podrá requerir documentación adicional para atender la solicitud para lo cual se cuentan con siete (7) días hábiles contados desde el día siguiente de la fecha de recepción de la 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.

Responsabilidad de respuesta en primera instancia: Oficial de Privacidad.

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: Si la información es insuficiente o errónea de forma que no permita su atención, se podrá requerir documentación adicional para atender la solicitud para lo cual se cuentan con siete (7) días hábiles contados desde el día siguiente de la fecha de recepción de la 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.

Responsabilidad de respuesta en primera instancia: Oficial de Privacidad.

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

- **Derecho de cancelación:** Solicitud para obtener la 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.

Consideraciones respecto del derecho de cancelación:

Subsanación: Si la información es insuficiente o errónea de forma que no permita su atención, se podrá requerir documentación adicional para atender la solicitud para lo cual se cuentan con siete (7) días hábiles contados desde el día siguiente de la fecha de recepción de la 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.

Responsabilidad de respuesta en primera instancia: Oficial de Privacidad.

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

- **Derecho de oposición**: Solicitud dirigida a requerir que no se lleve a cabo el Tratamiento de Datos Personales o cese su uso por no haber prestado su consentimiento.

Consideraciones respecto del derecho de oposición:

Subsanación Si la información es insuficiente o errónea de forma que no permita su atención, se podrá requerir documentación adicional para atender la solicitud para lo cual se cuentan con siete (7) días hábiles contados desde el día siguiente de la fecha de recepción de la 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.

Responsabilidad de respuesta en primera instancia: Oficial de Privacidad.

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

11) 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.

7. RESPONSABILIDADES

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

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 Privacidad 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.

OFICIAL DE CUMPLIMIENTO/OFICIAL DE PRIVACIDAD

El Oficial de Cumplimiento de la Empresa ejerce la función de Oficial de Privacidad 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.
- Nivel de especialización razonable en materia de protección de Datos Personales y Privacidad.

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.

COLABORADORES

- Conocer y cumplir las disposiciones de la presente Política.
- Solicitar orientación al Oficial de Privacidad 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 Privacidad 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 Privacidad cualquier incidente, o sospecha de incidente que considere afecte o pudiera afectar Datos Personales o la privacidad de alguna persona física.

GERENTES SUPERVISORES

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

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 Privacidad respecto a los controles de seguridad de la información y ciberseguridad relacionados a la LPDP.
- Informar al Oficial de Privacidad 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.

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 Privacidad 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 Privacidad 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 Privacidad respecto de los controles de seguridad física relacionados a la LPDP señalados en el anexo 2.

ÁREA LEGAL

- Atender a las consultas legales relacionadas a la protección de Datos Personales y privacidad.
- Atender los requerimientos del responsable Oficial de Privacidad respecto de los controles relacionados a las medidas legales de la LPDP descritas en el anexo 2.
- 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 Privacidad sobre los avances de las medidas legales implementadas para el cumplimiento de la LPDP en la Empresa.

8. EXCEPCIONES

En caso de presentarse excepciones y/o casos especiales en la presente política, el Oficial de Privacidad y el Gerente Legal y Gerente de TI revisarán y aprobarán las solicitudes, analizando los casos y los posibles riesgos que podrían presentarse.

9. ANEXOS

Ver de manera complementaria con el siguiente documento:

KALL-GRC-018-01 Listado de Anexos a la Política de Protección de Datos Personales