Política de Protección de Datos Personales

Contenido

CONTROL DE CAMBIOS

VERSION	FECHA DE APROBACION	DESCRIPCION DEL CAMBIO REALIZADO
1	Julio, 2016	Creación
2	Mayo, 2023	Ajuste de la razón social y actualización de información de contacto.

	Revisó	Aprobó
Nombre	Julian Manrique	Lina Montoya
Cargo	Coord. Legal	Dir. Legal & Asuntos Corporativos

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

1. Ámbito de aplicación

Prime Termovalle S.A.S. E.S.P. (la "Compañía") , con objeto de garantizar el adecuado cumplimiento de la Ley Estatutaria 1581 de 2012 de Protección de Datos (LEPD) y del Decreto 1377 de 2013, adopta esta política donde se establecen los procedimientos y normas para otorgar seguridad a los registros que contengan datos personales, con el fin de impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; adicionalmente, se establecen procedimientos a seguir para dar respuesta a las solicitudes de acceso y reclamos ejercitadas en virtud de los derechos de acceso, corrección, supresión, revocación o reclamo por infracción del titular de los datos personales objeto de tratamiento por la empresa.

Las disposiciones de esta política se aplican a las bases de datos personales objeto de responsabilidad de la Compañía, así como a los sistemas de información, soportes y equipos empleados en el tratamiento de los datos, que deban ser protegidos de acuerdo con la normativa vigente, a las personas que participan en el tratamiento y a los lugares donde se ubican dichas bases de datos.

2. Definiciones

2.1. **Acceso autorizado:** Autorización concedida a un usuario para el uso de determinados recursos. En dispositivos automatizados es el resultado de una autentificación correcta, generalmente mediante el ingreso de usuario y contraseña.

2.2. Autenticación: Procedimiento de verificación de la identidad de un usuario

2.3. Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

2.4. Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento.

2.5. Contraseña: Seña secreta que permite el acceso a dispositivos, información o bases de datos antes inaccesibles. Se utiliza en la autentificación de usuarios que permite el acceso autorizado**.**

2.6. Control de acceso: Mecanismo que permite acceder a dispositivos, información o bases de datos mediante la autentificación.

2.7. Copia de respaldo: Copia de los datos de una base de datos en un soporte que permita su recuperación

2.8. Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

2.9. **Dato privado:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

2.10. **Dato semiprivado:** Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

2.11. **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

2.12. **Identificación:** Proceso de reconocimiento de la identidad de los usuarios.

2.13. **Incidencia:** Cualquier anomalía que afecte o pueda afectar a la seguridad de los datos, constituyendo un riesgo para la confidencialidad, disponibilidad o integridad de las bases de datos o de los datos personales que contienen.

2.14. **Perfil de usuario:** Grupo de usuarios a los que se da acceso.

2.15. **Recurso protegido:** Cualquier componente del sistema de información, como bases de datos, programas, soportes o equipos, empleados para el almacenamiento y tratamiento de datos personales.

2.16. **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

2.17. **Responsable de seguridad:** Una o varias personas designadas por el responsable del tratamiento para el control y la coordinación de las medidas de seguridad.

2.18. **Sistema de información:** Conjunto de bases de datos, programas, soportes y/o equipos empleados para el tratamiento de datos personales.

2.19. **Soporte:** Material en cuya superficie se registra información o sobre el cual se pueden guardar o recuperar datos, como el papel, la cinta de video, el CD, el DVD, el disco duro, etc.

2.20. **Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento.

2.21. **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

2.22. **Usuario:** Sujeto autorizado para acceder a los datos o recursos, o proceso que accede a los datos o recursos sin identificación de un sujeto.

3. Principios del tratamiento de datos personales:

El artículo 4 de la Ley de Protección de Datos (LEPD), establece unos principios para el tratamiento de datos personales que se han de aplicar, de manera armónica e integral, en el desarrollo, interpretación y aplicación de la Ley. Los principios legales de la protección de datos son los siguientes:

- **Principio de legalidad:** El tratamiento de los datos es una actividad reglada que debe sujetarse a lo establecido en la Ley de Protección de Datos (LEPD), el Decreto 1377 de 2013 y en las demás disposiciones que la desarrollen.

- **Principio de finalidad:** El tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

- **Principio de libertad:** El tratamiento solo puede ejercerse con el consentimiento previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que revele el consentimiento. El tratamiento de los datos requiere la autorización previa e informada del Titular por cualquier medio que permita ser consultado con posterioridad, salvo en los siguientes casos que exceptúa el artículo 10 de la Ley de Protección de Datos (LEPD):

    - Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
    - Datos de naturaleza pública.
    - Casos de urgencia médica o sanitaria.
    - Tratamiento de información autorizado por la Ley para fines históricos, estadísticos o científicos.
    - Datos relacionados con el Registro Civil de las personas.

- **Principio de veracidad o calidad:** La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

- **Principio de transparencia:** En el tratamiento debe garantizarse el derecho del Titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan. En el momento de solicitar la autorización al titular, el responsable del tratamiento deberá informarle de manera clara y expresa lo siguiente, conservando prueba del cumplimiento de este deber:

    - El tratamiento al cual será sometidos sus datos y la finalidad del mismo.
    - El carácter facultativo de la respuesta del Titular a las preguntas que le sean hechas cuando éstas traten sobre datos sensibles o sobre datos de niños, niñas o adolescentes.
    - Los derechos que le asisten como Titular.
    - La identificación, dirección, correo electrónico y teléfono del responsable del tratamiento.

- **Principio de acceso y circulación restringida:** El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la Ley de Protección de Datos (LEPD) y la Constitución. En este sentido, el tratamiento solo podrá hacerse por personas

autorizadas por el titular y/o por las personas previstas en la Ley. Los datos personales, salvo la información pública, no podrán estar disponibles en internet y otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los titulares o terceros autorizados conforme a la Ley.

- **Principio de seguridad:** La información sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. El responsable del tratamiento tiene la responsabilidad de implantar las medidas de seguridad correspondientes y de ponerlas en conocimiento todo personal que tenga acceso, directo o indirecto, a los datos. Los usuarios que accedan a los sistemas de información del responsable del tratamiento deben conocer y cumplir con las normas y medidas de seguridad que correspondan a sus funciones. Cualquier modificación de las normas y medidas en materia de seguridad de datos personales por parte del responsable del tratamiento ha de ser puesta en conocimiento de los usuarios.

- **Principio de confidencialidad:** Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la LEPD y en los términos de la misma.

4. Categorías especiales de datos:

4.1 Datos sensibles

Los datos sensibles son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

4.2 Tratamiento de datos sensibles

Según el artículo 6 de la LEPD, se prohíbe el tratamiento de datos sensibles, excepto cuando:

- El Titular haya dado su autorización explícita 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 éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
- El tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular.
- 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. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los titulares.

4.3 Derechos de los niños, niñas y adolescentes

El tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, y cuando dicho tratamiento cumpla con los siguientes requisitos:

- Que responda y respete el interés superior de los niños, niñas y adolescentes.
- Que se asegure el respeto de sus derechos fundamentales

Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor a su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás.

Todo responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos, cumpliendo en todo momento con los principios y obligaciones recogidos en la LEPD y el Decreto 1377 de 2013. En todo caso, el tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.

Los derechos de acceso, corrección, supresión, revocación o reclamo por infracción sobre los datos de los niños, niñas adolescentes se ejercerán por las personas que estén facultadas para representarlos.

5. Tratamiento y finalidades de las bases de datos:

La Compañía, en el desarrollo de su actividad empresarial, lleva a cabo el tratamiento de datos personales relativos a personas naturales que están contenidos y son tratados en bases de datos destinadas a finalidades legítimas, cumpliendo con la Constitución y la Ley.

La siguiente tabla presenta las distintas bases de datos que manejan la empresa y las finalidades asignadas a cada una de ellas:

BASE DE DATOS	FINALIDAD	DESCRIPCIÓN FINALIDAD
Proveedores	Gestión contable, fiscal y administrativa - Gestión de proveedores y contratistas.	Solicitud de ofertas y propuestas económicas para la adquisición de productos y servicios; para el análisis y viabilidad de cada producto y/o servicio; envío de comunicaciones a través de mensajes de texto y correos electrónico; presentación de informes pertinentes a los diferentes entes de control; revisión y verificación de referencias comerciales; gestiones pre contractuales y contractuales; suministro de información en procesos de auditoría interna y externa que se realicen al interior de la institución; envío de información de los productos, servicios o novedades de la fundación; rastreo en bases de datos restrictivas tales como (policía, procuraduría, contraloría, SAGRILAFT – Sistema de Administración de Riesgo de Lavado de Activos y Financiación del Terrorismo y las demás que la normatividad colombiana disponga); cerco epidemiológico; las anteriores finalidades son enunciativas y no taxativas.
Trabajadores	Gestionar todo lo relativo a los datos personales con la actividad de la empresa, tales como nómina y prestaciones sociales.	Gestionar todo lo relativo con los datos personales con la actividad de la empresa, tales como nómina, condiciones de salud y prestaciones sociales gestionar todo lo relativo con los datos personales con la actividad de la empresa, tales como nómina y prestaciones sociales.

Visitantes	Finalidades varias - Registro de entrada y salida de documentos	Los datos serán utilizados con las siguientes finalidades. Autorizar la entrada a las diferentes áreas o dependencias de la institución; envío de información en mensajes de texto y correos electrónico con motivos promocionales y/o informativos; las anteriores finalidades son enunciativas y no taxativas.
Vigilancia Biométrica	Seguridad - Seguridad	Los datos serán utilizados con las siguientes finalidades: monitoreo y control para la vigilancia de entrada, salida y tráfico de personas dentro de la institución, así como para el control de ingreso y salida de vehículos de los parqueaderos, monitoreo y control de la prestación de los servicios institucionales.

6. Datos de navegación que usan datos personales

El sistema de navegación y el software necesario para el funcionamiento de la página web recogen algunos datos personales, cuya transmisión se halla implícita en el uso los protocolos de comunicación de Internet.

Por su propia naturaleza, la información recogida podría permitir la identificación de usuarios a través de su asociación con datos de terceros, aunque no se obtenga para ese fin. En esta categoría de datos se encuentran, la dirección IP o el nombre de dominio del equipo utilizado por el usuario para acceder a la página web, la dirección URL, la fecha y hora y otros parámetros relativos al sistema operativo del usuario.

Estos datos de utilizan con la finalidad exclusiva de obtener información estadística anónima sobre el uso de la página web o controlar su correcto funcionamiento técnico, y se cancelan inmediatamente después de ser verificados.

El acceso a datos personales a través de redes de comunicaciones, públicas o privadas, debe someterse a medidas de seguridad equivalentes al acceso local de datos personales.

La transmisión de datos personales mediante redes públicas o inalámbricas de comunicaciones electrónicas se tiene que llevar a cabo cifrando dichos datos, o utilizando otro mecanismo similar que garantice que la información no sea inteligible ni manipulada por terceras personas.

Cookies o Web Bugs

El sitio web no utiliza cookies o web bugs para recabar datos personales del usuario, sino que su utilización se limita a facilitar al usuario el acceso a la página web. El uso de cookies de sesión, no memorizadas de forma permanente en el equipo del usuario y que desaparecen cuando cierra el navegador, únicamente se limitan a recoger información técnica para identificar la sesión con la finalidad de facilitar el acceso seguro y eficiente de la página web. Si no desea permitir el uso de cookies puede rechazarlas o eliminar las ya existentes configurando su navegador, e inhabilitando el código Java Script del navegador en la configuración de seguridad.

7. Responsable del tratamiento de la información:

El responsable del tratamiento de las bases de datos objeto de esta política es la Compañía, cuyos datos son los siguientes:

PRIME TERMOVALLE S.A.S. E.S.P., NIT 805003351- 4, con sede principal en Kilometro 6 vía Yumbo – Aeropuerto Zona Franca del Pacifico de la ciudad de Palmira, conmutador +57 602 2801047, correo electrónico datospersonales@prime-energia.com

8. Medidas de seguridad

La Compañía con el fin de cumplir con el principio de seguridad consagrado en el artículo 4 literal g) de la LEPD, ha implementado medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Por otra parte, la Compañía mediante la suscripción de los correspondientes contratos de transmisión, ha requerido a los encargados del tratamiento con los que trabaje, la implementación de las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de la información en el tratamiento de los datos personales.

9. Autorización del titular

De acuerdo con el artículo 9 de la LEPD, para el tratamiento de datos personales se requiere la autorización previa e informada del titular. Mediante la aceptación de la presente política, todo titular que facilite información relativa a sus datos personales está consintiendo el tratamiento de sus datos por parte de la Compañía en los términos y condiciones recogidos en la misma.

No será necesaria la autorización del titular cuando se trate de:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.

- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las personas.

10. Derechos de los titulares:

De acuerdo con el Artículo 8 de la ley de Protección de Datos Personales 1581 de 2012, a los Artículos 21 y 22 del Decreto 1377 de 2013 y a los artículos 15 y 20 de la Constitución Política, los titulares de los datos pueden ejercer una serie de derechos en relación con el tratamiento de sus datos personales (conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en archivos o bases de datos).

Estos derechos podrán ejercerse por las siguientes personas:

1. Por el Titular, quién deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.
2. Por sus causahabientes, quienes deberán acreditar tal calidad.
3. Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.
4. Por estipulación a favor de otro y para otro.

Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

Los derechos del titular son los siguientes:

1. **Derecho de acceso o consulta:** Se trata del derecho del titular a ser informado por el responsable del tratamiento, previa solicitud con respecto al origen, uso y finalidad que se le han dado a sus datos personales.

2. **Derechos de quejas y reclamos:** La Ley distingue cuatro tipos de reclamos:
   - Reclamo de corrección: El derecho del titular a que se actualicen, rectifiquen o modifiquen aquellos datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
   - Reclamo de supresión: El derecho del titular a que se supriman los datos que resulten inadecuados, excesivos o que no respeten los principios, derechos y garantías constitucionales y legales.
   - Reclamo de revocación: El derecho del titular a dejar sin efecto la autorización previamente prestada para el tratamiento de sus datos personales.
   - Reclamo de infracción: El derecho del Titular a solicitar que se subsane el incumplimiento de la normativa en materia de Protección de Datos.

3. **Derecho a solicitar prueba de la autorización otorgada al responsable del tratamiento:** salvo cuando expresamente se exceptúe como requisito para el tratamiento de conformidad con lo previsto en el artículo 10 de la ley de Protección de Datos Personales (LEPD).

4. **Derecho a presentar ante la Superintendencia de Industria y Comercio quejas por infracciones:** el Titular o causahabiente solo podrá elevar esta queja una vez haya agotado el trámite de consulta o reclamo ante el responsable del tratamiento o encargado del tratamiento.

11. Procedimiento para ejercer los derechos del titular

El Titular de los datos puede ejercitar el derecho de acceso, consulta o reclamo sobre sus datos a través de los siguientes canales:

- Correo electrónico: datospersonales@prime-energia.com
- Correspondencia física, a la dirección Km 6 vía Yumbo – Aeropuerto Zona Franca del Pacífico.
- Vía telefónica: teléfono +57 602 2801047

A la solicitud se deberán adjuntar los siguientes documentos:

- Fotocopia de la cédula de ciudadanía del titular y de la persona que lo representa (si es el caso), así como del documento acreditativo de tal representación.

- Documentos acreditativos de la petición formulada que se quieran hacer valer, cuando corresponda.

11.1. Consultas:

Según el artículo 21 del Decreto 1377 de 2013, el Titular podrá consultar de forma gratuita sus datos personales en dos casos:

- Al menos una vez cada mes calendario.

- Cada vez que existan modificaciones sustanciales de las políticas de tratamiento de la información que motiven nuevas consultas.

Para consultas cuya periodicidad sea mayor a una por cada mes calendario, la Compañía solamente podrá cobrar al Titular gastos de envío, reproducción y, en su caso, certificación de documentos. Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente. Para tal efecto, el responsable deberá demostrar a la Superintendencia de Industria y Comercio, cuando ésta así lo requiera, el soporte de dichos gastos.

Tiempos de respuesta de acuerdo con el artículo 14 de la ley de protección de datos:

Una vez recibida la solicitud, la Compañía resolverá la petición de consulta en un plazo máximo de diez (10) días hábiles contados a partir de la fecha de recibo de esta.

Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

11.2. Reclamos:

Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas.

Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga “reclamo en trámite” y el motivo de este, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

Tiempos de respuesta de acuerdo con el artículo 14 de la ley de protección de datos:

La Compañía resolverá la petición de consulta en un plazo máximo de quince (15) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender al reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

Una vez agotado el trámite de consulta o reclamo, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

12. Deberes de los responsables del tratamiento y encargados del tratamiento

12.1. Funciones y obligaciones del personal

Todas las personas que intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con los datos personales y sistemas de información de la Compañía, deben actuar de conformidad con las funciones y obligaciones recogidas en el presente manual y en las políticas de Seguridad de la Información y Ciberseguridad.

Todas las bases de datos deberán registrarse ante el Registro Nacional de Base de Datos administrador por la Superintendencia de Industria y Comercio.

La Compañía debe informar a su personal de servicio, de las medidas y normas de seguridad que competen al desarrollo de sus funciones, así como de las consecuencias de su incumplimiento, mediante cualquier medio de comunicación que garantice su recepción o difusión (correo electrónico, carteleras, etc.).

De igual modo, debe poner a disposición del personal el presente manual para que puedan conocer la normativa de seguridad de la empresa y sus obligaciones en esta materia, en función del cargo que ocupan.

La Compañía cumple con el deber de información, con la inclusión de acuerdos de confidencialidad y deber de secreto que suscriben, en su caso, los usuarios de sistemas que contengan Datos Personales.

Las funciones y obligaciones del personal de la Compañía se definen, con carácter general, según el tipo de actividad que desarrollan dentro de la empresa y, específicamente, por el contenido de este manual. Con carácter general, cuando un usuario trate documentos o soportes que contienen datos personales, tiene el deber de custodiarlos, así como de vigilar y controlar que personas no autorizadas puedan tener acceso a ellos.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en este manual, por parte del personal al servicio de la Compañía, es sancionable de acuerdo con la normativa aplicable a la relación jurídica existente entre el usuario y la empresa.

Las funciones y obligaciones de los usuarios de las bases de datos personales bajo responsabilidad de la Compañía, son las siguientes:

- **Deber de secreto:** Aplica a todas las personas que, en el desarrollo de su profesión o trabajo, acceden a bases de datos personales y vincula tanto a usuarios de la Compañía como a los prestadores de servicios contratados. En cumplimiento de este deber, los usuarios no pueden comunicar o revelar a terceras personas, datos que manejen o de los que tengan conocimiento en el desempeño o cargo de sus funciones y deben velar por la confidencialidad e integridad de los mismos.

- **Funciones de control y autorizaciones delegadas:** El responsable del tratamiento de datos puede delegarlo a terceros, para que actúen como encargados, mediante un contrato de transmisión de datos. Cuando se firmen contratos de transmisión de datos, estos estarán registrados en el inventario de contratos administrados por la Jefatura de Asuntos Legales.

- **Obligaciones relacionadas con las medidas de seguridad implantadas:**
  - Acceder a las bases de datos solamente con la debida autorización y cuando sea necesario para el ejercicio de sus funciones.
  - No revelar información a terceras personas ni a usuarios no autorizados.
  - Observar las normas de seguridad y trabajar para mejorarlas.

- No realizar acciones que supongan un peligro para la seguridad de la información.
- No sacar información de las instalaciones de la organización sin la debida autorización.

- Uso de recursos y materiales de trabajo: Debe estar orientado al ejercicio de las funciones asignadas. No se autoriza el uso de estos recursos y materiales para fines personales o ajenos a las tareas correspondientes al puesto de trabajo. Cuando, por motivos justificados de trabajo, sea necesaria la salida de dispositivos periféricos o extraíbles, deberá comunicarse a los responsables de seguridad que podrán autorizarla y, en su caso, registrarla.

- Uso de impresoras, escáneres y otros dispositivos de copia: Cuando se utilicen este tipo de dispositivos debe procederse a la recogida inmediata de las copias, evitando dejar éstas en las bandejas de los mismos.

- Obligación de notificar incidencias: Los usuarios tienen la obligación de notificar a los responsables de seguridad, las incidencias de las que tengan conocimiento, quienes se encargarán de su gestión y resolución. Algunos ejemplos de incidencias son: la caída del sistema de seguridad informática que permita el acceso a los datos personales a personas no autorizadas, el intento no autorizado de la salida de un documento o soporte, la pérdida de datos o la destrucción total o parcial de soportes, el cambio de ubicación física de bases de datos, el conocimiento por terceras personas de contraseñas, la modificación de datos por personal no autorizado, etc.

- Deber de custodia de los soportes utilizados: Obliga al usuario autorizado a vigilar y controlar que personas no autorizadas accedan a la información contenida en los soportes. Los soportes que contienen bases de datos deben identificar el tipo de información que contienen mediante un sistema de etiquetado y ser inventariados. Cuando la información esté clasificada con nivel de seguridad sensible el sistema de etiquetado solo debe ser comprensible para los usuarios autorizados a acceder a dicha información.

- Responsabilidad sobre los terminales de trabajo y portátiles: Cada usuario es responsable de su propio terminal de trabajo; cuando esté ausente de su puesto, debe bloquear dicho terminal (ej. protector de pantalla con contraseña) para impedir la visualización o el acceso a la información que contiene y tiene el deber de apagar el terminal al finalizar la jornada laboral. Asimismo, los ordenadores portátiles han de estar controlados en todo momento para evitar su pérdida o sustracción.

- Uso limitado de Internet y correo electrónico: El envío de información por vía electrónica y el uso de Internet por parte del personal está limitado al desempeño de sus actividades en la empresa.

- Salvaguarda y protección de contraseñas: Las contraseñas proporcionadas a los usuarios son personales e intransferibles, por lo tanto se prohíbe su divulgación o comunicación a personas no autorizadas. Cuando el usuario accede por primera vez con la contraseña asignada es necesario

que la cambie. Cuando sea necesario restaurar la contraseña, el usuario debe comunicarlo al administrador del sistema.

- Copias de respaldo y recuperación de datos: Debe realizarse copia de seguridad de toda la información de bases de datos personales de la empresa.
- Deber de archivo y gestión de documentos y soportes: Los documentos y soportes deben de ser debidamente archivados con las medidas de seguridad establecidas por el proceso de Gestión Documental.

12.2. Responsable del tratamiento de los datos personales

El responsable del tratamiento de datos personales es quién tiene decisión sobre las bases de datos que los contengan.

Las obligaciones en materia de seguridad de los datos de la Compañía, son las siguientes:

- Coordinar e implantar las medidas de seguridad recogidas en el Manual de Políticas de Seguridad de la Información y Ciberseguridad.
- Difundir el referido documento al personal que le aplique.
- Mantener el Manual de Políticas de Seguridad de la Información y Ciberseguridad actualizado y revisado siempre que se produzcan cambios relevantes en el sistema de información, el sistema de tratamiento, la organización de la empresa, el contenido de la información de las bases de datos, o como consecuencia de los controles periódicos realizados. De igual modo, se revisará su contenido cuando se produzca algún cambio que pueda afectar al cumplimiento de las medidas de seguridad.
- Designar uno o más responsables de seguridad e identificar a los usuarios autorizados para acceder a las bases de datos que contienen datos personales.
- Cuidar que el acceso a sistemas y aplicaciones informáticas se lleve a cabo mediante el uso de sistemas de autenticación.
- Autorizar, salvo delegación expresa a usuarios autorizados, la salida de los medios donde se encuentran las bases de datos.
- Verificar semestralmente la correcta aplicación del procedimiento de copias de respaldo y recuperación de datos.
- Garantizar la existencia de una lista de usuarios autorizados y perfiles de usuario.
- Analizar al menos cada tres meses, junto con la Coordinación de Riesgos y Cumplimiento, las incidencias registradas para establecer las medidas correctivas oportunas.
- Realizar una auditoría, interna o externa, para verificar el cumplimiento de las medidas de seguridad en materia de protección de datos, al menos cada año.
- El responsable del tratamiento de datos puede delegarlo a terceros, para que actúen como encargados del tratamiento, mediante un contrato de transmisión de datos.

12.3. Encargado de la seguridad de los datos personales

Los encargados de seguridad tienen las siguientes funciones:

- Coordinar y controlar la implantación de las medidas de seguridad y colaborar con el responsable del tratamiento en la difusión del Manual Interno de Seguridad.
- Coordinar y controlar los mecanismos que permiten acceder a la información contenida en las bases de datos y elaborar un informe periódico sobre dicho control.
- Gestionar los permisos de acceso a los datos por parte de los usuarios autorizados identificados en el Manual Interno de Seguridad.
- Gestionar las incidencias relacionadas con la seguridad de los datos, de acuerdo con la política de Gestión de incidentes cibernéticos o de seguridad de la información.
- Comprobar periódicamente, la validez y vigencia de la lista de usuarios autorizados, la existencia y validez de las copias de seguridad para la recuperación de los datos, la participación en la actualización de normas de seguridad de la información y ciberseguridad y el cumplimiento de las medidas relacionadas con las entradas y salidas de datos.
- Definir los tiempos dentro de los cuales se realizarán las auditorías, los cuales no podrán ser superiores a dos años.
- Recibir y analizar el informe de auditoría para elevar sus conclusiones y proponer medidas correctoras al responsable del tratamiento.
- Gestionar y controlar los registros de entradas y salidas de documentos o soportes que contengan datos personales.

13. Transferencia de datos a terceros países

De acuerdo con el Título VIII de la LEPD, se prohíbe la transferencia de datos personales a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios. Esta prohibición no regirá cuando se trate de:

- Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.
- Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del Titular por razones de salud o higiene pública.
- Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.
- Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.
- Transferencias necesarias para la ejecución de un contrato entre el Titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.
- Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

En los casos no contemplados como excepción, corresponderá a la Superintendencia de Industria y Comercio proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. El Superintendente está facultado para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

Las transmisiones internacionales de datos personales que se efectúen entre un responsable y un encargado para permitir que el encargado realice el tratamiento por cuenta del responsable, no requerirán ser informadas al Titular ni contar con su consentimiento, siempre que exista un contrato de transmisión de datos personales.

14. Vigencia

Las bases de datos bajo la responsabilidad de la Compañía serán objeto de tratamiento durante el tiempo que sea razonable y necesario para la finalidad, para la cual son recabados los datos. Una vez cumplida la finalidad o finalidades del tratamiento, y sin perjuicio de normas legales que dispongan lo contrario, la Compañía procederá a la supresión de los datos personales en su posesión, salvo que exista una obligación legal o contractual que requiera su conservación. Por todo ello, dicha base de datos ha sido creada sin un periodo de vigencia definido.

La presente política de tratamiento permanece vigente desde el julio de 2016.

15. Disposición Final

El presente manual ha sido aprobado por la Compañía como responsable del tratamiento de datos, en julio de 2016, aceptando su contenido, ordenando su ejecución y cumplimiento con carácter general, por todo el personal de la empresa, y en particular, por aquellos a los referidos en este documento.