MARPICO S.A.S.

Política para el Tratamiento de Datos Personales

Bogotá, Octubre 2025

Tabla de Contenido

1. INTRODUCCIÓN 4
2. OBJETIVO 4
3. ALCANCE 4
4. DESTINATARIOS 5
5. DEFINICIONES 5
6. POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES 6
7. RESPONSABLE Y ENCARGADO DEL TRATAMIENTO DE DATOS 7
8. DEBERES DE LA EMPRESA COMO RESPONSABLE DEL TRATAMIENTO 8
9. DERECHOS DE LOS TITULARES 9
10. TRATAMIENTO Y FINALIDADES DEL USO DE LA INFORMACIÓN 10
10.1. Bases de datos de trabajadores 10
10.2. Bases de datos de Clientes 11
10.3. Bases de datos de Proveedores 12
10.4. Bases de datos de archivos Inactivos 13
10.5. Tratamiento de Datos de Imágenes 14
10.6. Tratamiento de datos personales para fines de Marketing y Publicidad 14
10.7. Tratamiento de las fotos como datos personales 15
11. CATEGORIAS ESPECIALES DE DATOS 15
11.1. Datos Sensibles 15
11.2. Autorización Especial de Datos Personales Sensibles 16
11.3. Derechos de Niños, Niñas y Adolescentes 16
12. AUTORIZACIÓN POR PARTE DE LOS TITULARES 17
12.1. Casos en que no es Necesaria la Autorización 18
13. ACCIONES GENERALES PARA LA PROTECCIÓN DE DATOS PERSONALES 18
13.1. Tratamiento de la Información 18
13.2. Uso de la Información 18
13.3. Almacenamiento de Información 19
13.4. Destrucción 19
13.5. Procedimiento de Gestión de Incidentes con Datos Personales 20
14. ÁREA RESPONSABLE DE LA ATENCIÓN A PETICIONES, CONSULTAS Y RECLAMOS 22
15. PROCEDIMIENTO PARA ATENDER LOS DERECHOS DE LOS TITULARES 22
15.1. Procedimiento de Consultas 22

15.2. Procedimiento de Reclamos 23
15.3. Procedimiento de Supresión de Datos Personales:..... 25
16. CAPACITACIONES 25
17. PERIODO DE VIGENCIA DE LAS BASES DE DATOS..... 26
18. REGISTRO NACIONAL DE BASE DE DATOS..... 26
19. Contacto y Canales de Atención..... 26
20. VIGENCIA..... 26
21. CONTROL DE CAMBIOS 27

1. INTRODUCCIÓN

La Constitución Política de Colombia establece en el artículo 15 el derecho de protección de datos personales como el derecho de toda persona para conocer, actualizar, rectificar, y/o cancelar la información y datos personales que de ella se hayan recolectado y/o se traten en bases de datos públicas o privadas.

Mediante la Ley 1581 de 2012, el Congreso de la República reglamentó el mencionado derecho al establecer las Disposiciones Generales para la Protección de Datos Personales en Colombia, igualmente reglamentada por los Decretos 1377 de 2013 y 886 de 2014, hoy incorporados en el Decreto Único 1074 de 2015, entre otros.

En cumplimiento de las anteriores disposiciones, **MARPICO S.A.S.,** ha elaborado la presente **POLÍTICA PARA EL TRATAMIENTO DE DATOS PERSONALES**, cuya finalidad es establecer los lineamientos de la Empresa para el cumplimiento de las obligaciones legales en materia de protección de datos personales.

2. OBJETIVO

La presente Política tiene como objetivo dar la información necesaria y suficiente a los diferentes grupos de interés, así como establecer los lineamientos que garanticen la protección de los datos personales que son objeto de tratamiento de datos personales a través de los procedimientos de La Empresa, para de esta forma, dar cumplimiento a la Ley 1581 de 2012, los Decretos 1377 de 2013 y 886 de 2014, hoy incorporados en el Decreto Único 1074 de 2015, que desarrollan el derecho constitucional que tienen los titulares a conocer, actualizar y rectificar los datos personales registrados en las bases de datos o archivos de La Empresa.

3. ALCANCE

Dar un trámite expedito y legal a las diferentes solicitudes y reclamaciones hechas por los Titulares de la Información, así como por sus causahabientes u otra persona que cuente con la debida autorización.

Dar cumplimiento a las exigencias de la normatividad vigente en materia de Protección de Datos Personales.

Brindar la debida protección a los intereses y necesidades de los titulares de la información personal tratada por La Empresa.

4. DESTINATARIOS

Esta política se aplicará a todas las bases de datos tanto físicas como digitales, que contengan datos personales y que sean objeto de tratamiento por parte de La Empresa, considerada como responsable. Igualmente, en aquellos casos en que operen como encargada del tratamiento de datos personales.

La presente Política está dirigida a que los trabajadores, clientes, proveedores, y demás grupos de interés tengan a su disposición la información necesaria y suficiente sobre los diferentes tratamientos y fines sobre los que serán objeto sus datos, así como los derechos que ellos, como titulares de datos personales, pueden ejercer frente a La Empresa cuando esta tenga el rol de responsable del tratamiento de datos personales.

5. DEFINICIONES

- **ACCESO RESTRINGIDO:** Nivel de acceso a la información limitada a parámetros previamente definidos. La Empresa no hará disponibles Datos Personales para su acceso a través de Internet u otros medios de comunicación masiva, a menos que se establezcan medidas técnicas que permitan controlar el acceso y restringido solo a las personas Autorizadas.

- **AUTORIZACIÓN:** Es el consentimiento que da cualquier persona para que las empresas o personas responsables del tratamiento de la información, puedan utilizar sus datos personales.

- **AVISO DE PRIVACIDAD:** Es una de las opciones de comunicación verbal o escrita que brinda la ley para darle a conocer a los titulares de la información, la existencia y las formas de acceder a las políticas de tratamiento de la información y el objetivo de su recolección y uso.

- **BASE DE DATOS:** Conjunto organizado de datos personales que son objeto de tratamiento, incluye archivos físicos y electrónicos.

- **DATO PERSONAL:** Se trata de cualquier información vinculada o que pueda asociarse a una persona determinada, como su nombre o número de identificación, o que puedan hacerla determinable, como sus rasgos físicos.

- **DATO PRIVADO:** Es el dato que por su naturaleza íntima o reservada solo es relevante para el titular. Los gustos o preferencias de las personas, por ejemplo, corresponden a un dato privado.

- **DATO PÚBLICO:** Es uno de los tipos de datos personales existentes. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

- **DATO SEMIPRIVADO:** Son los datos que no tienen naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo al titular sino a cierto sector o a la sociedad en general. Los datos financieros y crediticios de la actividad comercial o de servicios, son algunos ejemplos.

- **DATOS SENSIBLES:** Son aquellos que afectan la intimidad del titular o pueden dar lugar a que lo discriminen, es decir, aquellos que revelan su origen racial o étnico, su orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos, entre otros.

- **DERECHO DE LOS NIÑOS, NIÑAS Y ADOLESCENTES:** En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.

- **EMPRESA:** Hace referencia a MARPICO S.A.S., sociedad legalmente constituida, con domicilio principal en Bogotá, D.C., e identificada con NIT. 800.015.615-7.

- **ENCARGADO DEL TRATAMIENTO:** Es la persona natural o jurídica que realiza el tratamiento de datos personales, a partir de una delegación que le hace el responsable, recibiendo instrucciones acerca de la forma en la que deberán ser administrados los datos.

- **GRUPOS DE INTERÉS:** Son personas y organizaciones que están interesadas e involucradas con La Empresa que usted representa e interactúan con la misma.

- **RESPONSABLE DEL TRATAMIENTO:** Es la 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. La Empresa actúa como responsable del tratamiento de datos personales frente a todos los datos personales sobre los cuales decida directamente, en cumplimiento de las funciones propias reconocidas legalmente.

- **TITULAR:** Es la persona natural cuyos datos personales son objeto de tratamiento.

- **TRANSFERENCIA:** Se trata de la operación que realiza el responsable o el encargado del tratamiento de los datos personales, cuando envía la información a otro receptor, que, a su vez, se convierte en responsable del tratamiento de esos datos.

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

6. POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

MARPICO S.A.S., dando cumplimiento a la Ley 1581 de 2012, los Decretos 1377 de 2013 y 886 de 2014, hoy incorporados en el Decreto Único 1074 de 2015, actúa como Responsable de la recolección,

almacenamiento, uso, circulación y actualización de los datos personales que le han sido suministrados y autorizados de manera libre, previa, clara, expresa, voluntaria e informada por los titulares de la información y que reposan en las bases de datos de archivos físicos o digitales, bajo medidas técnicas, humanas y administrativas que garantizan la confidencialidad, veracidad y disponibilidad, evitando adulteración, pérdida, consulta, uso o acceso no autorizado.

7. RESPONSABLE Y ENCARGADO DEL TRATAMIENTO DE DATOS

MARPICO S.A.S., sociedad comercial legalmente constituida, identificada con el NIT.800.015.615-7, con domicilio principal en la Calle 100 No. 8 A 49 Torre B Oficina 702 de la ciudad de Bogotá D.C., Colombia.

Página www.ranger.com.co; www.marpicopromocionales.com; www.marpicovinos.com;, www.clubdelcatador.com

Teléfono 601-6235566.

Igualmente son responsables del tratamiento de los datos personales por Área los siguientes:

- **TRABAJADORES**
  Área Responsable:
  Gerente de Gestión Humana

- **CLIENTES**
  Áreas Responsables:
  División de Promocionales: Director de la División de Promocionales – Gerente Comercial – Jefe de Cartera.
  División de Vinos & Licores: Director de la División de Vinos & Licores, Gerente Comercial - Gerente de Mercadeo - Jefe de Cartera.
  División de Ferretería: Director de la División de Ferretería - Gerente Comercial – Jefe de Cartera.

- **CLIENTES DE COMERCIO ELECTRÓNICO**
  Áreas Responsables:
  Jefe de Desarrollo / Jefe de Seguridad Lógica
  División de Promocionales y Ferretería (Marpico 360º): Director de la División– Gerentes Comerciales – Gerente de Mercadeo Omnicanal – Jefe de Cartera
  División de Vinos & Licores: Director de la División de Vinos & Licores, Gerente Comercial - Gerente de Mercadeo - Jefe de Cartera.

- **PROVEEDORES NACIONALES**
  Áreas Responsables:
  Director General - Jefe de Contabilidad – Coordinadora de Tesorería - Coordinadora de Compras Nacionales – Administradores de Contrato.

- **PROVEEDORES DEL EXTERIOR**
  Áreas Responsables: Director General - Directores de Línea - Gerente de Compras Internacionales - Jefe de Contabilidad – Jefe de Importaciones - Coordinadora de Tesorería.

- **SEGURIDAD LÓGICA (TECNOLOGÍA)**
  Jefe de Seguridad Lógica — responsable integral de la Política de Tratamiento de Datos Personales y de la seguridad de la información en la Empresa, así como responsable principal del sistema de videovigilancia (CCTV) en el ámbito tecnológico. Sus funciones comprenden la administración de la infraestructura tecnológica, la custodia y conservación de las grabaciones, el control y registro de accesos, la gestión de solicitudes internas, la atención de requerimientos de autoridades competentes, la coordinación de reportes de incidentes ante la SIC, la implementación de controles técnicos de seguridad y la supervisión de las capacitaciones en materia de protección de datos.

8. DEBERES DE LA EMPRESA COMO RESPONSABLE DEL TRATAMIENTO

A continuación, se describen los deberes de La Empresa**,** en el tratamiento de los datos personales:

a. Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
b. Solicitar autorización al titular de la información para el tratamiento de sus datos personales, informándole sobre la finalidad de la recolección y los derechos que le asisten en virtud de la autorización otorgada.
c. Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten en virtud de la autorización otorgada.
d. Conservar la información bajo las condiciones de marketing necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
e. Garantizar que la información que se suministre al encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
f. Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a éste se mantenga actualizada.
g. Rectificar la información cuando sea incorrecta y comunicar lo pertinente al encargado del tratamiento.
h. Suministrar al encargado del tratamiento, según el caso, únicamente datos cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la ley.
i. Exigir al encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular.
j. Tramitar las consultas y reclamos formulados en los términos señalados en la ley.
k. Informar al encargado del tratamiento cuando determinada información se encuentra en discusión por parte del titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

l. Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
m. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.
n. Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
o. Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley.
p. Actualizar la información reportada por los responsables del tratamiento dentro de los ocho (8) días hábiles contados a partir de su recibo.
q. Tramitar las consultas y los reclamos formulados por los titulares dentro de los diez (10) días hábiles contados a partir de su recibido.
r. Registrar en la base de datos la leyenda "reclamo en trámite".
s. Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
t. Abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
u. Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
v. Inscribir en el Registro Nacional de Bases de Datos, de manera independiente, cada una de las bases de datos que contengan datos personales sujetos a Tratamiento.

9. DERECHOS DE LOS TITULARES

Como titular de sus datos personales Usted tiene derecho a:

a. Acceder de forma gratuita a los datos proporcionados que hayan sido objeto de tratamiento.
b. Conocer, actualizar y rectificar su información frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté prohibido o no haya sido autorizado.
c. Solicitar prueba de la autorización otorgada.
d. Presentar ante la Superintendencia de Industria y Comercio (SIC) quejas por infracciones a lo dispuesto en la normatividad vigente.
e. Revocar la autorización y/o solicitar la supresión del dato, siempre que no exista un deber legal o contractual que impida eliminarlos.
f. Abstenerse de responder las preguntas sobre datos sensibles. Tendrá carácter facultativo las respuestas que versen sobre datos sensibles o sobre datos de las niñas y niños y adolescentes.

10. TRATAMIENTO Y FINALIDADES DEL USO DE LA INFORMACIÓN

De acuerdo con lo establecido en la Ley 1581 de 2012 y de conformidad con las autorizaciones impartidas por los titulares de la información, La Empresa realizará operaciones o conjunto de operaciones que incluyen recolección de datos, su almacenamiento, uso circulación y/o supresión. Este tratamiento de datos se realizará exclusivamente para as finalidades autorizadas y previstas en la presente Política en las autorizaciones especificas otorgadas por parte del titular.

De la misma forma se realizará Tratamiento de datos Personales cuando exista una obligación legal o contractual para ello, siempre bajo los lineamientos de la Política de Seguridad de la Información de La Empresa.

En la ejecución del objeto social de La Empresa, los datos personales serán tratados de acuerdo con el grupo de interés y en proporción a la finalidad o finalidades que tenga cada tratamiento, como se describe a continuación:

10.1. Bases de datos de trabajadores

Son las bases de datos tanto físicas como digitales que contienen datos personales de los trabajadores, que incluyen:
Datos generales de identificación del trabajador, familiares, beneficiarios, incluidos, los hijos menores, Datos específicos de identificación del trabajador (firma, nacionalidad), Datos biométricos del trabajador (huella, fotografías, videos), Datos relacionados con actividad profesional del trabajador, Datos de ubicación personal relacionados con actividad privada, Datos relacionados con el estado de salud del trabajador, Datos de preferencias, identidad y orientación sexual del trabajador, origen étnico-racial, etc, Identificación de trabajadores pertenecientes a poblaciones vulnerables, Datos sobre trabajadores en situación de discapacidad (origen común y origen laboral), Datos financieros del trabajador, Datos socioeconómicos del trabajador, Datos de información tributaria del trabajador , Datos patrimoniales del trabajador, Datos relacionados con historia laboral del trabajador, Datos relacionados con el nivel educativo del trabajador, Datos relacionados con afiliación y aportes al Sistema Integral de Seguridad Social del trabajador, Datos de antecedentes judiciales y disciplinarios del trabajador.

El tratamiento tiene como finalidad:

- Dar cumplimiento a las obligaciones de ley y contractuales contraídas con el Titular de la Información;
- Efectuar el pago de salarios, prestaciones sociales, auxilios, indemnizaciones y aportes a la seguridad social;
- Afiliar al trabajador y sus beneficiarios al sistema general de seguridad social, los datos personales de menores serán tratados con la finalidad de dar cumplimiento a las obligaciones legales;
- Suministrar información que puede ser de interés del trabajador, tales como, convenios a planes exequiales, planes complementarios, medicina prepagada, ofrecer programas de

bienestar corporativo y planificar actividades empresariales, para el titular y sus beneficiarios;

- Los datos biométricos capturados a través de sistemas de videovigilancia o grabación su tratamiento tendrá como finalidad la identificación, seguridad y la prevención de fraude interno y externo, llevar a cabo todos los procedimientos de seguridad establecidos por la empresa, tales como videos de vigilancia, toma de huellas dactilares para el acceso a las oficinas, expedición del carnet y/o facilidades donde la misma opera;
- El desarrollo de eventuales investigaciones con el fin de dar cumplimiento al reglamento interno del trabajo,
- El reporte de información a las autoridades competentes;
- La supervisión y monitoreo de herramientas tecnológicas y correo electrónicos corporativos;
- La consolidación de bases de datos, y la generación de copias y archivos de seguridad de la información en los equipos proporcionados por la empresa;
- En convocatorias de selección, los datos personales tratados tendrán como finalidad adelantar las gestiones de los procesos de selección; las hojas de vida se gestionarán garantizando el principio de acceso restringido;
- La administración del recurso humano, incluyendo procesos de capacitación, evaluación de desempeño y adelanto de programas de bienestar social y seguridad y salud en el trabajo;
- La adopción de medidas necesarias para brindar seguridad en el manejo de la información electrónica y física;
- Adelantar investigaciones internas de conformidad con las diferentes políticas de la empresa en caso de actividades sospechosas que puedan afectar el buen nombre de la empresa;
- Realizar todos los trámites internos y el cumplimiento de obligaciones contables, tributarias y de ley;
- Mantener un archivo físico o digital que permita contar con la información correspondiere a cada contrato laboral;
- En general, las demás actividades requeridas para desarrollar el objeto social de la empresa, establecidos en su Política para el Tratamiento de Datos Personales.

En esta base de datos, se incorpora información privada, pública, datos sensibles y de menores. El tratamiento de los datos para los fines diferentes a las obligaciones derivadas de la relación laboral requerirá autorización previa del titular o su representante legal, según sea el caso.

10.2. Bases de datos de Clientes

Son las bases tanto físicas como digitales que contienen datos de las personas naturales y jurídicos, que mantienen un vínculo contractual y comercial, cuyo tratamiento tiene como finalidad:

- Para todos los fines relacionados con el objeto social de la Empresa, contractuales o relacionados con éstos;
- Cumplir con las disposiciones legales y contractuales para la venta de productos;
- Realizar todos los trámites internos y el cumplimiento de obligaciones contables, tributarias y de ley;
- Realizar invitaciones a eventos y ofrecer nuevos productos;

- Contactar al titular o sus dependientes a través de cualquier medio electrónico – SMS o chat para el envío de información comercial;
- Efectuar encuestas de satisfacción respecto de los bienes ofrecidos por la empresa;
- Suministrar información de contacto a la fuerza comercial y/o red de distribución, telemercadeo, investigación de mercados y cualquier tercero con el cual la empresa, tenga un vínculo contractual para el desarrollo de actividades de ese tipo (investigación de mercados y telemercadeo, etc.) y para la ejecución de las mismas;
- Contactar al Titular o sus dependientes a través de medios telefónicos para realizar encuestas, estudios y/o confirmación de datos personales necesarios para la ejecución de una relación contractual;
- Contactar al Titular o sus dependientes a través de medios electrónicos – SMS o chat para el envío de noticias relacionadas con campañas de fidelización o mejora de servicio;
- Contactar al Titular o sus dependientes a través de correo electrónico, WhatsApp, teléfono, celular para la gestión de la cartera en relación con las obligaciones derivadas del contrato celebrado entre las partes;
- Realizar visitas al establecimiento de comercio o dirección señalada por el cliente como domicilio comercial, verificación de referencias;
- Suministrar la información a terceros con los cuales la empresa, tenga relación contractual y que sea necesario entregársela para el cumplimiento del objeto contratado;
- El reporte de información a las autoridades competentes;
- La consolidación de bases de datos, y la generación de copias y archivos de seguridad de la información;
- La adopción de medidas necesarias para brindar seguridad en el manejo de la información electrónica y física;
- Adelantar investigaciones internas de conformidad con las diferentes políticas de la empresa en caso de actividades sospechosas que puedan afectar el buen nombre de la empresa; y,
- Mantener un archivo físico o digital que permita contar con la información correspondiere de cada cliente;
- En general, las demás actividades requeridas para desarrollar el objeto social de la empresa, establecidos en su Política para el Tratamiento de Datos Personales.

Esta base de datos contiene datos personales públicos y privados, los cuales tienen como finalidad el desarrollo de relaciones contractuales. El tratamiento de estos datos para fines diferentes al mantenimiento de la relación contractual o el cumplimiento de deberes de carácter legal requiere de autorización previa del titular.

10.3. Bases de datos de Proveedores

Son las bases de datos tanto físicas como digitales que contienen datos de las personas naturales y jurídicas que mantienen un vínculo contractual y comercial, cuyo tratamiento tiene como finalidad:

- Para todos los fines relacionados con el objeto de los procesos de selección de proveedores, contractuales o relacionados con éstos;

- Realizar todos los trámites internos y el cumplimiento de obligaciones contables, tributarias y de ley;
- Realizar todas las actividades necesarias para el cumplimiento de las diferentes etapas contractuales en las relaciones con proveedores y contratistas;
- Para las adquisiciones de servicios y bienes requeridos por La Empresa;
- Para su normal funcionamiento o el cumplimiento de algunas de sus funciones;
- Efectuar las gestiones pertinentes para el desarrollo del objeto social de la empresa en lo que tiene que ver con el cumplimiento del objeto del contrato celebrado con el Titular de la información;
- Suministrar la información a terceros con los cuales la empresa, tenga relación contractual y que sea necesario entregársela para el cumplimiento del objeto contratado;
- El reporte de información a las autoridades competentes;
- La consolidación de bases de datos, y la generación de copias y archivos de seguridad de la información;
- La adopción de medidas necesarias para brindar seguridad en el manejo de la información electrónica y física;
- Adelantar investigaciones internas de conformidad con las diferentes políticas de la empresa en caso de actividades sospechosas que puedan afectar el buen nombre de la empresa;
- Mantener un archivo físico o digital que permita contar con la información correspondiere a cada contrato;
- En general, las demás actividades requeridas para desarrollar el objeto social de la empresa, establecidos en su Política para el Tratamiento de Datos Personales.

Esta base de datos contiene datos personales públicos y privados, los cuales tienen como finalidad el desarrollo de relaciones contractuales. El tratamiento de estos datos para fines diferentes al mantenimiento de la relación contractual o el cumplimiento de deberes de carácter legal requiere de autorización previa del titular.

10.4. Bases de datos de archivos Inactivos

Son las bases de datos manuales o sistematizadas que contienen archivos o información de carácter personal inactiva. Esta información se encuentra almacenada, garantizando su disponibilidad, la localización exacta, su integridad, la confidencialidad y trazabilidad de la información. La administración y conservación de la información de carácter personal almacenada en estas bases de datos, tendrá como finalidad el cumplimiento de sus obligaciones.

Sin perjuicio de lo anterior, los titulares de datos personales almacenados en estas bases de datos podrán ejercer en cualquier momento sus derechos de conocer, actualizar y rectificar sus datos, a solicitar prueba de esta autorización, a presentar quejas ante la Superintendencia de Industria y Comercio, revocar la autorización y/o solicitar la supresión de algún dato, y a acceder en forma gratuita a sus datos personales.

10.5. Tratamiento de Datos de Imágenes

La Empresa cuenta con sistemas de videovigilancia operativos las veinticuatro (24) horas del día, ubicados en diferentes áreas de sus instalaciones. La finalidad es garantizar la seguridad de personas, bienes, mercancías, equipos e instalaciones, y prevenir, detectar o apoyar investigaciones sobre incidentes que afecten la integridad física, patrimonial o el normal desarrollo de actividades.

El tratamiento se realiza conforme a los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad. No se utilizarán imágenes para fines distintos ni se instalarán cámaras en zonas con expectativa de privacidad (baños, vestidores, zonas de descanso).

Se informará mediante avisos visibles la existencia de cámaras, la finalidad, la identificación del responsable y el contacto. Las imágenes se conservarán solo por el tiempo estrictamente necesario y se eliminarán de forma segura, salvo obligación legal o requerimiento de autoridad. El acceso a grabaciones estará restringido y su entrega a terceros se hará únicamente a autoridades competentes con solicitud formal.

Responsabilidad operativa (Tecnología): El Jefe de Seguridad Lógica actuará como responsable principal del sistema de videovigilancia en el ámbito tecnológico, incluyendo (i) administración de la plataforma y equipos, (ii) custodia y conservación de grabaciones dentro de los plazos definidos, (iii) control y registro de accesos a las imágenes, (iv) atención de solicitudes internas debidamente autorizadas y (v) respuesta a requerimientos de autoridades, garantizando la cadena de custodia cuando corresponda.

10.6. Tratamiento de datos personales para fines de Marketing y Publicidad

Es fundamental establecer si es estrictamente necesario que la información que se va a utilizar para proyectos de marketing, mercadotecnia y publicidad debe ir asociada o referirse a una persona. De no ser así, se utilizará información anonimizada de tal manera que no se pueda identificar al Titular del dato.

El uso de los datos personales para actividades de publicidad u ofrecimiento de productos y servicios se realice en días y horarios que no afecten la paz ni intimidad familiar, el horario usual de descanso, ni desconozcan su “derecho a la tranquilidad”

Es fundamental establecer si es estrictamente necesario que la información que se va a utilizar para proyectos de comercio electrónico debe ir asociada o referirse a una persona. De no ser así, se recomienda se utilizará la información anonimizada de tal manera que no se pueda identificar al Titular del dato.

10.7. Tratamiento de las fotos como datos personales

Son las bases de datos que contienen fotografías, cuyo tratamiento tiene como finalidad la Publicidad y Marketing para la venta de nuestros productos.

Para la toma de una fotografía o si se contrata a un tercero para que tome fotografías debe estar autorizado por el titular del dato (persona fotografiada), mediante formato **074-** AutorizacionUsoDeImagenPersonaMayorDeEdad y para menores de edad mediante el formato **075-** AutorizacionUsoDeImagenMenorDeEdad. En caso de no adquirirse las fotos directamente del titular, si no que le son siniestradas por terceros, debe asegurarse de:

- Las fotografías se obtuvieron lícitamente
- El tercero cuenta con autorización para suministrarle las fotografías y ser utilizadas para los fines específicos.

Téngase presente que los menores de edad son Titulares del derecho de Protección de Datos Personales. El representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto. 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.

Esta información se protege de acuerdo con las siguientes medidas en La Empresa: Control de Carpetas que contiene la información de niños, niñas y adolescentes. El control de las carpetas está a cargo del Área de Comercial y Ventas.

11. CATEGORIAS ESPECIALES DE DATOS

11.1. Datos Sensibles

Se entiende por datos sensibles 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 pertenecía 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.

Tratamiento de datos sensibles:
En nuestra empresa, está prohibido la recolección, almacenamiento, uso y circulación de los datos sensibles, excepto en los siguientes aspectos:

- 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 proteger 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 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.

A continuación, se establecen los siguientes controles asegurando la prohibición del tratamiento de datos sensibles:

- Está prohibido realizar exámenes que puedan revelar información de la que se pueda discriminar al trabajador (VIH y embarazo); Al ser datos sensibles no es obligación suministrarlos y puede considerarse una práctica discriminatoria.
- No se realizan preguntas en el proceso de selección que no sean relevantes para definir el perfil profesional del aspirante al cargo como por ejemplo condición sexual, antecedentes de haber sufrido acoso laboral, convicciones religiosas, filosóficas y políticas.

11.2. Autorización Especial de Datos Personales Sensibles

La Empresa informará a través de los diversos medios de obtención de la autorización a todos sus titulares, que en virtud de la ley 1581 de 2012 y normas reglamentarias estos no están obligados a otorgar la autorización para el tratamiento de datos sensibles.

En caso de tratamiento de datos relativos a la salud, La Empresa implementará las medidas necesarias para proteger la confidencialidad de la información. Los datos sensibles biométricos tratados tienen como finalidad la identificación de las personas, la seguridad, el cumplimiento de obligaciones legales y la adecuada prestación de los productos.

11.3. Derechos de Niños, Niñas y Adolescentes

El tratamiento de los datos personales de niño, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, y cuando dicho tratamiento cumpa con los siguientes parámetros y/o requisitos:

- Que respondan y respeten 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 de los niños, niñas y adolescentes otorgará la autorización.

- La Empresa se asegurará que en el tratamiento de la información el respeto a los derechos de niños, niñas y adolescentes. La información de niños, niñas y adolescentes se utiliza para lo siguiente:
  - Durante la entrevista se indaga sobre los datos básicos de los hijos de los trabajadores (Nombre, edad y a que se dedica), esta información se utiliza para realizar el perfil familiar del trabajador.
  - En la inclusión de los beneficiarios menores de edad para la EPS y la Caja de Compensación Familiar los siguientes datos: (Nombres y Apellidos, Número de Identificación, Fecha de Nacimiento, Sexo, Nivel Educativo y Dirección de Residencia).
  - Para actividades de bienestar para el núcleo familiar, donde hacen parte los hijos de los trabajadores, la siguiente información: Nombres, Apellidos y Edad.

Esta información se protege de acuerdo con las siguientes medidas: Control de Carpetas que contiene la información de niños, niñas y adolescentes. El control de las carpetas está exclusivamente a cargo del Área de Gestión Humana.

12. AUTORIZACIÓN POR PARTE DE LOS TITULARES

Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior. Se entenderá que la autorización cumple con estos requisitos cuando se manifieste (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del Titular que permiten concluir de forma razonable que otorgo la autorización, como cuando, por ejemplo, se remite a La Empresa una hoja de vida para participar en procesos de selección o cuando se ingresa a las instalaciones de la Empresa a sabiendas de la existencia de sistemas de videovigilancia.

a. **TRABAJADORES:** Al iniciar el proceso de selección, debe hacer firmar del aspirante el “Formato de autorización de tratamiento de datos personales”. En la etapa de contratación, se incluye dentro del contrato de trabajo la cláusula de tratamiento de datos personales.

b. **CLIENTES:** Cuando se inicia una relación comercial, se firma el “Formulario de solicitud de crédito” o “Formulario de conocimiento del cliente”, el cual incluye la autorización expresa de tratamiento de datos personales.

c. **PROVEEDORES:** Cuando se inicia una relación comercial con un proveedor nacional, se firma el “Formulario Único conocimiento de proveedores Nacionales”, el cual incluye la autorización expresa para el tratamiento de datos personales.

   Cuando se inicia o durante la relación comercial, se firma con el proveedor internacional el formulario “International Suppliers Form”, el cual incluye la autorización expresa de tratamiento de datos personales.

d. **FOTOGRAFÍAS:** Para la toma de una fotografía o si se contrata a un tercero para que tome fotografías debe estar autorizado por el titular del dato (persona fotografiada), mediante formato **074-**AutorizacionUsoDeImagenPersonaMayorDeEdad y para menores de edad mediante el formato **075-**AutorizacionUsoDeImagenMenorDeEdad.

12.1. Casos en que no es Necesaria la Autorización

La autorización del Titular no será necesaria cuando se trate de:

- Información requerida por alguna 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 autorizada por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las personas.

Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la Ley 1581 de 2012 y demás normas concordantes y vigentes.

13. ACCIONES GENERALES PARA LA PROTECCIÓN DE DATOS PERSONALES

A continuación, se establecen los lineamientos generales aplicados por La Empresa con el fin de cumplir con sus obligaciones en cumplimiento de los principios para la administración de datos personales.

13.1. Tratamiento de la Información

Todos los Trabajadores de La Empresa, al realizar las actividades propias de su cargo, asumirán las responsabilidades y las obligaciones que se tienen en el manejo adecuado de la información personal, desde su recolección, almacenamiento, uso, circulación y hasta su disposición final.

13.2. Uso de la Información

La información de carácter personal contenida en las bases de datos debe ser utilizada y tratada de acuerdo con las finalidades descritas en la presente política.

En caso de que algún área identifique nuevos usos diferentes a los descritos en la presente Política de Tratamiento de Datos Personales, deberá informar al Jefe de Seguridad Lógica, quien evaluará y gestionará, cuando aplique, su inclusión en la presente política.

Igualmente, se deben tomar en consideración los siguientes supuestos:

- En caso de que un área diferente de la que recolectó inicialmente el dato personal requiera utilizar los datos personales que se han obtenido, ello se podrá hacer siempre que se trate de un uso previsible por el tipo de servicios que ofrece La Empresa y para una finalidad contemplada dentro de la presente Política de Tratamiento de Datos Personales.
- Cada área debe garantizar que en las prácticas de reciclaje de documentos físicos no se divulgue información confidencial ni datos personales. Por lo anterior, no se podrán reciclar hojas de vida, ni títulos académicos, ni certificaciones académicas o laborales, ni resultados de exámenes médicos ni ningún documento que contenga información que permita identificar a una persona.
- En caso de que un encargado haya facilitado datos personales o bases de datos a algún área para un fin determinado, el área que solicitó los datos personales no debe utilizar dicha información para una finalidad diferente de la relacionada en la Política de Tratamiento de Datos Personales; al finalizar la actividad, es deber del área que solicitó la información, eliminar la base de datos o los datos personales utilizados evitando el riesgo de desactualización de información o casos en los cuales durante ese tiempo un titular haya presentado algún reclamo.
- Los Trabajadores no podrán tomar decisiones que tengan un impacto significativo en la información personal, o que tengan implicaciones legales, con base exclusivamente en la información que arroja el sistema de información, por lo que deberán validar la información a través de otros instrumentos físicos o de manera manual, y, si es necesario, de manera directa por parte del titular del dato, en los casos en que así sea necesario.
- Únicamente los Trabajadores autorizados pueden introducir, modificar o anular los datos contenidos en las bases de datos o documentos objeto de protección. Los permisos de acceso de los usuarios son concedidos por el Área de Seguridad Lógica, de acuerdo con los perfiles establecidos, los cuales serán previamente definidos por los líderes de los procesos donde se requiera el uso de información personal.
- Cualquier uso de la información diferente al establecido, será previamente consultado con el Jefe de Seguridad Lógica.

13.3. Almacenamiento de Información

El almacenamiento de la información digital y física se realiza en medios o ambientes que cuentan con adecuados controles para la protección de los datos. Esto involucra controles de seguridad física e informática, tecnológicos y de tipo ambiental en áreas restringidas, en instalaciones propias y/o centros de cómputo o centros documentales gestionados por terceros.

13.4. Destrucción

La destrucción de medios físicos y electrónicos se realiza a través de mecanismos que no permiten su reconstrucción. Se realiza únicamente en los casos en que no constituya el desconocimiento de norma legal alguna, dejando siempre la respectiva trazabilidad de la acción.

La destrucción comprende información contenida en poder de terceros como en instalaciones propias.

13.5. Procedimiento de Gestión de Incidentes con Datos Personales

En caso de presentarse un incidente de seguridad que afecte o pueda afectar la confidencialidad, integridad o disponibilidad de los datos personales, el Jefe de Seguridad Lógica deberá informar el hecho a la Delegatura de Protección de Datos Personales de la Superintendencia de Industria y Comercio (SIC) dentro de los quince (15) días hábiles siguientes al conocimiento del incidente, conforme a lo dispuesto en la Circular Externa 01 de 2022.

El informe deberá incluir como mínimo: la descripción del incidente, tipo de datos comprometidos, número de titulares afectados, medidas adoptadas y plan de acción para mitigar los impactos.

Las incidencias pueden afectar tanto a bases de datos digitales como físicas y generarán las siguientes actividades:

a. Notificación de Incidentes

Cuando se presuma que un incidente pueda afectar o haber afectado a bases de datos con información personal datos personales se deberá informar al Jefe de Seguridad Lógica quién gestionará su reporte en el Registro Nacional de Bases de Datos.

b. Gestión de Incidentes

Es responsabilidad de cada trabajador, contratista, consultor o tercero, reportar de manera oportuna cualquier evento sospechoso, debilidad o violación de políticas que pueden afectar la confidencialidad, integridad y disponibilidad de los activos e información personal de La Empresa.

c. Identificación

Todos los eventos sospechosos o anormales, tales como aquellos en los que se observe el potencial de perdida de reserva o confidencialidad de la información, deben ser evaluados para determinar si son o no, un incidente y deben ser reportados al nivel adecuado en La Empresa. Cualquier decisión que involucre a las autoridades de investigación y judiciales debe ser hecha en conjunto entre el Jefe de Seguridad Lógica y la Gerencia Jurídica. La comunicación con dichas autoridades será realizada por ellos mismos.

d. Reporte

Todos los incidentes y eventos sospechosos deben ser reportados tan pronto como sea posible a través de los canales internos establecidos por La Empresa.

Si la información sensible o confidencial es perdida, divulgada a personal no autorizado o se sospecha de alguno de estos eventos, el Jefe de Seguridad Lógica, debe ser notificado de forma inmediata.

Los Trabajadores deben reportar a su jefe directo y al Jefe de Seguridad Lógica cualquier daño o pérdida de computadores o cualquiera otro dispositivo, cuando estos contengan datos personales en poder de La Empresa.

A menos que exista una solicitud de la autoridad competente debidamente razonada y justificada, ningún Trabajador debe divulgar información sobre sistemas de cómputo, y redes que hayan sido afectadas por un delito informático o abuso de sistema. Para la entrega de información o datos en virtud de orden de autoridad, la Gerencia Jurídica deberá intervenir con el fin de prestar el asesoramiento adecuado.

e. Contención, Investigación y Diagnostico

El Jefe de Seguridad Lógica debe garantizar que se tomen acciones para investigar y diagnosticar las causas que generaron el incidente, así como también debe garantizar que todo el proceso de gestión del incidente sea debidamente documentado.

En caso de que se identifique un delito informático, en los términos establecidos en la Ley 1273 de 2009, el Jefe de Seguridad Lógica y la Gerencia Jurídica, reportaran tal información a las autoridades de investigaciones judiciales respectivas.

Durante los procesos de investigación se deberá garantizar la "Cadena de Custodia" con el fin de preservarla en caso de requerirse establecer una acción legal.

f. Solución

El Área de Seguridad Lógica, así como cualquier área comprometida y los directamente responsables de la gestión de datos personales, deben prevenir que el incidente de seguridad se vuelva a presentar, corrigiendo todas las vulnerabilidades existentes.

g. Cierre de Incidente y Seguimiento

El Área de Seguridad Lógica y las áreas que usan o requieren la información, iniciarán y documentarán todas las tareas de revisión de las acciones que fueron ejecutadas para remediar el incidente de seguridad.

El Jefe de Seguridad Lógica preparará un análisis anual de los incidentes reportados. Las conclusiones de este informe se utilizarán en la elaboración de campañas de concientización que ayuden a minimizar la probabilidad de incidentes futuros.

h. Reporte de incidentes ante la SIC como autoridad de control

Se reportarán como novedades los incidentes de seguridad que afecten la base de datos, de acuerdo con las siguientes reglas:

- En la parte inferior del menú de cada base de datos registrada en el sistema, se presentan dos (2) opciones para informar las novedades:

  - ✓ La violación de los códigos de seguridad o la pérdida, hurto y/o acceso no autorizado de información de una base de datos administrada por el Responsable del Tratamiento o por su Encargado, deberán reportarse al Registro Nacional de Bases de Datos dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos.

- ✓ Los líderes de proceso reportarán de forma interna los incidentes asociados a datos personales ante el Jefe de Seguridad Lógica, quién dentro del plazo legal procederá a reportarlos ante el Registro Nacional de Bases de Datos.

14. ÁREA RESPONSABLE DE LA ATENCIÓN A PETICIONES, CONSULTAS Y RECLAMOS

Las peticiones, consultas y reclamos formulados por los titulares de Datos Personales bajo Tratamiento de La Empresa para ejercer sus derechos a conocer, actualizar, rectificar y suprimir datos, o revocar la autorización deberán ser dirigidas a:

Jefe de Seguridad Lógica: Calle 100 No. 8 A 49 Torre B Oficina 611 de Bogotá, D.C.
Teléfono: (601) 6235566 Ext. 122
Correo electrónico: habeasdata@marpico.com.co

El rol antes mencionado será el contacto de los titulares de Datos Personales, para todos los efectos previstos en esta Política.

15. PROCEDIMIENTO PARA ATENDER LOS DERECHOS DE LOS TITULARES

Los titulares de Datos Personales, sin importar el tipo de vinculación que tengan con La Empresa, pueden ejercer sus derechos a conocer, actualizar, rectificar y suprimir información y/o revocar la autorización otorgada.

15.1. Procedimiento de Consultas

La Empresa, garantiza a los titulares de datos personales contenidos en sus bases de datos o a sus causahabientes o personas autorizadas, el derecho de consultar toda la información contenida en su registro individual o toda aquella que esté vinculada con su identificación conforme se establece en la presente Política.

Responsable de atención de consultas:
Jefe de Seguridad Lógica, será el responsable de recibir y dar trámite a las solicitudes remitidas, en los términos, plazos y condiciones establecidos en la Ley 1581 de 2012 y en la presente política.

Las consultas dirigidas a La Empresa deberán contener como mínimo la siguiente información:

a. Nombres y apellidos del Titular y/o su representante y/o causahabientes;
b. Lo que se pretende consultar

c. Dirección física, electrónica y teléfono de contacto del Titular y/o sus causahabientes o representantes;
d. Firma, número de identificación o procedimiento de validación correspondiente.
e. Haber sido presentada por los medios de consulta habilitados por La Empresa.

Una vez sea recibida la solicitud de CONSULTA de información por parte del Titular de los datos o su representante o tercero debidamente autorizado, a través de los canales establecidos por La Empresa, quien procederá a verificar que la solicitud contenga todas las especificaciones requeridas a efectos de poder valorar que el derecho se ejerza por un interesado o por un representante de éste, acreditando con ello, que se cuenta con la legitimidad legal para hacerlo.

15.1.1. Plazos de Respuesta a consultas:

Las solicitudes recibidas mediante los anteriores medios serán atendidas en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recibo.

15.1.2. Prórroga del plazo de Respuesta:

En caso de imposibilidad de atender la consulta dentro de dicho término, se informará al interesado antes del vencimiento de los diez (10) días, 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 plazo.

15.2. Procedimiento de Reclamos

Derechos Garantizados mediante el procedimiento de reclamos:

- Corrección o Actualización: La empresa y/o los Encargados, garantizarán a los titulares de datos personales contenidos en sus bases de datos o a sus causahabientes, el derecho de corregir o actualizar los datos personales que reposen en sus bases de datos, mediante presentación de reclamación, cuando consideren que se cumplen los parámetros establecidos por la ley o los señalados en la presente Política para que sea procedente la solicitud de Corrección o Actualización.
- Revocatoria de la autorización o Supresión de los datos Personales: La Empresa y/o los Encargados, garantizarán a los titulares de datos personales contenidos en sus bases de datos o a sus causahabientes, el derecho de Solicitar la Revocatoria de la autorización o solicitar la supresión de la información contenida en su registro individual o toda aquella que esté vinculada con su identificación cuando consideren que se cumplen los parámetros establecidos por la ley o los señalados en la presente Política. Así mismo se garantiza el derecho de presentar reclamos cuando adviertan el presunto incumplimiento de la Ley 1581 de 2012 o de la presente Política.

15.2.1. Responsable de atención de Reclamos:

El Jefe de Seguridad Lógica, será el responsable de recibir y dar trámite a las solicitudes remitidas, en los términos, plazos y condiciones establecidos en la Ley 1581 de 2012 y en la presente política.

Las reclamaciones presentadas deberán contener como mínimo la siguiente información:

- Nombres y apellidos del Titular y/o su representante y/o causahabientes;
- Lo que se pretende consultar**;**
- Dirección física, electrónica y teléfono de contacto del Titular y/o sus causahabientes o representantes;
- Firma, número de identificación o procedimiento de validación correspondiente**;**
- Haber sido presentada por los medios de consulta habilitados por La Empresa.

Una vez sea recibida la solicitud de ACTUALIZACIÓN o de RECTIFICACIÓN de información por parte del Titular de los datos o su representante o tercero debidamente autorizado, a través de los canales establecidos por La Empresa, el Área de Seguridad Lógica, quien procederá a verificar que la solicitud contenga todas las especificaciones requeridas a efectos de poder valorar que el derecho se ejerza por un interesado o por un representante de éste, acreditando con ello, que se cuenta con la legitimidad legal para hacerlo.

15.2.2. Reclamaciones sin cumplimiento de Requisitos legales:

En caso de que la reclamación se presente sin el cumplimiento de los anteriores requisitos legales, se solicitará al reclamante dentro de los cinco (5) días siguientes a la recepción del reclamo, para que subsane las fallas y presente la información o documentos faltantes.

15.2.3. Desistimiento del Reclamo:

Transcurrido **UN MES** desde la fecha del requerimiento sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

15.2.4. Recepción de reclamos que no correspondan a la Empresa:

En caso de que La Empresa reciba un reclamo dirigido a otra organización, informará en un término máximo de dos (2) días hábiles contados desde la recepción al reclamante sobre la imposibilidad de tramitar su reclamo.

15.2.5. Inclusión de leyenda en la base de datos:

Recibida la reclamación de forma completa, en un término máximo de dos (2) días hábiles contados desde la recepción, La Empresa Incluirá en la base de datos donde se encuentren los datos personales del Titular, una leyenda que diga "reclamo en trámite" y el motivo del mismo. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

15.2.6. Plazos de Respuesta a los Reclamos:

El término máximo para atender el reclamo será de quince (**15**) días hábiles contados a partir del día siguiente a la fecha de su recibo.

15.2.7. Prórroga del plazo de Respuesta:

Cuando no fuere posible atender el 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.

15.2.8. Requisito De Procedibilidad

El titular sólo podrá elevar queja ante la Superintendencia de Industria y Comercio (SIC), una vez haya agotado el trámite de consulta o reclamo ante nuestra empresa.

15.3. Procedimiento de Supresión de Datos Personales:

En caso de resultar procedente la Supresión de los datos personales del titular de la base de datos conforme a la reclamación presentada, La Empresa, deberá realizar operativamente la supresión de tal manera que la eliminación no permita la recuperación de la información, sin embargo, el Titular deberá tener en cuenta que en algunos casos cierta información deberá permanecer en registros históricos por cumplimiento de deberes legales de la empresa por lo que su supresión versará frente al tratamiento activo de los mismos y de acuerdo a la solicitud del titular.

16. CAPACITACIONES

La Empresa desarrollará e implementará programas anuales de capacitación y concientización en Protección de Datos Personales y Seguridad de la Información, en cumplimiento de lo dispuesto en la Ley 1581 de 2012, el Decreto 1377 de 2013 y las políticas internas adoptadas.

El Área de Seguridad Lógica será la responsable principal de la planeación, ejecución, actualización y seguimiento de dichos programas, asegurando que los trabajadores, contratistas y terceros comprendan sus deberes, responsabilidades, medidas de protección y consecuencias legales derivadas del tratamiento indebido de datos personales o de incidentes de seguridad de la información.

Los contenidos de los programas de formación serán revisados y actualizados periódicamente por el Área de Seguridad Lógica, teniendo en cuenta los cambios normativos, tecnológicos o jurisprudenciales aplicables.

El Área de Gestión Humana será responsable de informar de manera general a los nuevos trabajadores, al momento de su ingreso, sobre los lineamientos institucionales en materia de Protección de Datos Personales y Seguridad de la Información, y coordinará con el Área de Seguridad Lógica su participación en las capacitaciones formales.

Por su parte, el Área de Compras deberá informar a los contratistas sobre estas obligaciones al momento de su vinculación, y gestionar, junto con el Área de Seguridad Lógica, su inclusión en los procesos de capacitación y concientización establecidos por la Empresa.

Toda capacitación deberá contar con el correspondiente registro de asistencia y constancia de conocimiento por parte del personal capacitado.

17. PERIODO DE VIGENCIA DE LAS BASES DE DATOS

Las Bases de Datos de La Empresa tendrán el periodo de vigencia que corresponda a la finalidad para el cual se autorizó su tratamiento y de las normas especiales que regulen la materia.

18. REGISTRO NACIONAL DE BASE DE DATOS

De conformidad con el artículo 25 de la Ley 1581 de 2012 y sus decretos reglamentarios, La Empresa registrará sus bases de datos junto con la presente Política en el Registro Nacional de Bases de Datos (RNBD) administrado por la SIC.

La Empresa actualizará el RNBD anualmente o cuando se produzcan cambios sustanciales en la finalidad, responsable, encargado, canales de atención o estructura de las bases de datos, en cumplimiento del artículo 2.2.2.26.3.1 del Decreto 1074 de 2015.

19. Contacto y Canales de Atención

Responsable de atención de peticiones, consultas y reclamos: Jefe de Seguridad Lógica
Dirección: Calle 100 No. 8 A 49 Torre B Oficina 611, Bogotá D.C.
Teléfono: (601) 6235566 Ext. 122
Correo electrónico: habeasdata@marpico.com.co

Este será el canal único para el ejercicio de los derechos de los titulares de datos personales.

20. VIGENCIA

La presente Política de Tratamiento de Datos Personales rige a partir del 16 de junio de 2016, con vigencia indefinida.

Cualquier cambio sustancial en la Política de Tratamiento de Datos Personales, se comunicará de forma oportuna a los titulares de los datos a través de los medios habituales de contacto y/o a través de nuestros sitios web.

Para los titulares que no tengan acceso a medios electrónicos o aquellos a los que no sea posible contactar, se comunicará a través de avisos abiertos en la sede principal de la empresa.

21. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS			
Aspectos que cambiar en el documento	Responsable de la solicitud del cambio	Fecha del cambio DD/MM/AAAA	Versión
Actualización general de la política Cambio de formato	Eliana Fernández	15 enero 2021	01
Cambio de logo corporativo Cambio pie de página (de estar en todas las hojas a estar en la última) Actualización de políticas de acuerdo a las estipuladas por el Gobierno	Juliana Devia Eliana Fernández	06 abril 2022	02
Cambio de logo corporativo. Actualización de finalidades del uso de la información	Juliana Devia Eliana Fernández	01 diciembre 2023	03
Actualización Introducción, Objetivo, Alcance, Destinatarios Definiciones, Finalidades, Categorías Especiales de Datos, Acciones Generales para la Protección de Datos Personales, Procedimiento para Atender los Derechos de los Titulares, Capacitaciones, Vigencia, Registro de las Bases de Datos	Juliana Devia Eliana Fernández	08 de marzo de 2024	04
Actualización	Juliana Devia Eliana Fernández	29 de marzo de 2024	05
Actualización Base de datos Clientes	Juliana Devia Eliana Fernández	30 de julio de 2024	06
Se actualizan las responsabilidades asignadas al Área de Tecnología, las cuales pasan al Área de Seguridad Lógica	Daniel Quintero	23 de octubre de 2025	07