Política de Tratamiento de Datos Personales y Protección de Datos

Contenido

Anexos adicionales:

1. Objetivo:

La presente política se expide en cumplimiento de la Ley 1581 del 2012, Decreto 1074 de 2015, Ley 1266 de 2008, y de conformidad al Título V de la Circula Única de la Superintendencia de Industria y Comercio, sobre el régimen de protección de datos personales y busca garantizar que **GTM COLOMBIA S.A.,** en adelante **"CALDIC",** en condición de responsable de datos personales, realice el tratamiento en estricto cumplimiento de la normatividad aplicable, garantizando los derechos de los titulares de los datos.

Esta Política ofrece una introducción a las leyes de protección de datos personales, y cómo mitigar el riesgo de infringirlas, la cual será aplicable a todas las actividades de **CALDIC** en Colombia, por lo tanto, se espera que todos los empleados, contratistas, proveedores y clientes conozcan esta política y actúen de acuerdo con ella en todo momento **CALDIC** se compromete a establecer los procesos necesarios para cumplir todas las normas enunciadas, así como acatar los lineamientos del grupo **CALDIC** en la materia.

2. Definiciones

A efectos de la presente Política, las siguientes palabras y expresiones tendrán el significado que se indica a continuación:

Dato Personal Ley 1581 de 2012: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Dato Personal Ley 1266 de 2008: Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica.

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

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.

Encargado del Tratamiento: Persona Natural o Jurídica, pública o privada que por sí mismo o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

Titular: Persona natural cuyos datos personales son objeto de Tratamiento.

Tratamiento: Es cualquier actividad que implique el uso de datos personales. Incluye la recolección, almacenamiento, uso, circulación o supresión y cualquier operación realizada con datos personales, ya sea por medios automatizados o no.

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

Semiprivado: Se considera semiprivado aquel dato que no posee carácter confidencial, reservado ni público, y cuyo acceso o divulgación puede ser de interés no solo para su titular, sino también para un sector específico, un grupo determinado de personas o incluso para la sociedad en general.

Dato Público: Es aquel dato que no se clasifica como semiprivado, privado o sensible. Se consideran datos públicos, entre otros, aquellos relacionados con el estado civil de las personas, su ocupación o

actividad profesional, y su condición de comerciante o servidor público. Por su naturaleza, los datos públicos pueden encontrarse, entre otros, en registros oficiales, documentos públicos, gacetas, boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sujetas a reserva.

Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación.

Transferencia de datos: Tiene lugar cuando el Responsable del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del tratamiento y se encuentra dentro o fuera del país.

Transmisión de Datos: Tratamiento de datos personales que implica la comunicación de estos dentro o fuera del territorio de la República de Colombia, con el objeto de que un Encargado realice tratamiento por cuenta del responsable.

Ley 1952 de 2019 - Derecho De Los Niños, Niñas Y Adolescentes: En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes. Sólo podrán tratarse aquellos datos que sean de naturaleza pública.

Personal: incluye a todos nuestros empleados a tiempo completo y parcial, funcionarios, directores, consultores, empleados temporales, contratistas, voluntarios, empleados de agencias y colocaciones y otros usuarios de datos.

RNBD: El Registro Nacional de Bases de Datos (RNBD) es un sistema establecido por la Superintendencia de Industria y Comercio (SIC), diseñado para reportar la información relacionada con las bases de datos que las empresas, obligadas por la normativa vigente, administren.

GDPR: Significa el Reglamento General de Protección de Datos (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (entrará en vigor a partir del 25 de mayo de 2018).

Ley 1266 de 2008: Regula el tratamiento de datos personales relacionados con información financiera, crediticia, comercial y de servicios.

SIC: Significa Superintendencia de Industria y Comercio de Colombia (SIC) es la autoridad administrativa responsable de supervisar, vigilar y garantizar el cumplimiento de las normas relacionadas con la protección de datos personales.

3. Introducción a la legislación y la normativa sobre protección de datos

Toda persona tiene derechos sobre el tratamiento de sus datos personales. Durante nuestras actividades recopilamos, utilizamos, almacenamos y procesamos datos personales sobre nuestros empleados actuales, pasados y futuros, clientes, proveedores y otras terceras partes y otras personas con las que nos comunicamos.

Estos datos personales, que pueden conservarse en papel o en un ordenador u otro soporte, (es decir, en registros manuales o electrónicos), están sujetos a determinadas garantías legales especificadas: Ley 1581 del 2012, Decreto 1074 de 2015, Ley 1266 de 2008, titulo V circular unica SIC y demás legislación aplicable

sobre protección de datos en Colombia.

La presente Política establece las bases sobre las que trataremos los datos personales que obtengamos o que nos sean facilitados por empleados, colaboradores, proveedores, clientes, cualquier tercero y/o por otras fuentes, así como los requisitos de protección de datos que debemos cumplir tanto nosotros como nuestros usuarios de datos. Su objetivo es garantizar que cumplimos nuestras obligaciones legales en materia de protección de datos y que todo nuestro personal conoce nuestras obligaciones y lo que significan en la práctica. Esta política puede modificarse en cualquier momento.

Cada empleado es informado sobre la recogida y tratamiento de sus datos a través de nuestra Formulario de Consentimiento del Empleado sobre Privacidad de Datos (autorizacion para el tratamiento de datos). Los terceros son informados a través de los términos y condiciones, acuerdos de confidencialidad u otros contratos y autorizaciones.

Sólo recopilaremos y procesaremos datos de acuerdo con el consentimiento recibido. El consentimiento será voluntario en todo momento.

Es importante que cumplamos plenamente todos los requisitos aplicables en materia de protección de datos. Para garantizarlo, todo el personal debe cumplir esta Política, independientemente dese encuentre cumpliendo sus funciones.

4. Incumplimiento de la legislación y la normativa sobre protección de datos

No cumplir las leyes y normativas de protección de datos no es una opción.

El incumplimiento puede tener graves consecuencias, como multas sustanciales, medidas disciplinarias, incluido el despido del personal (sin preaviso o pago en lugar de preaviso), o la terminación del contrato de trabajo en caso de infracciones graves o reiteradas. Cuando se trate de conductas ilícitas por parte del personal (nos reservamos el derecho a informar de ello a las autoridades competentes) que puedan acarrear la responsabilidad personal del personal por sus acciones.

5. Responsable del tratamiento de datos personales

El responsable del tratamiento de los datos personales suministrados por los titulares de la información será **GTM COLOMBIA S.A**., persona jurídica de derecho privado, identificada con NIT 830.055.659-0, con domicilio principal en la ciudad de Bogotá D.C., y cuyos datos de contacto son los siguientes:

Dirección: Avenida Carrera 45 # 108 - 27 T 3, Piso 15, Bogotá D.C., Colombia
Página Web: https://www.caldic.com/es-co.
Correo electrónico: privacy_col@caldic.com

6. Principios de la Protección de Datos

Cualquiera que trate datos personales debe cumplir ciertos principios rectores aplicables contenidos en la Ley 1581 de 2012 y demás legislación aplicable, los cuales se resumen a continuación:

- **Principio de Legalidad:** El tratamiento de datos personales que realiza **CALDIC** es una actividad

regulada que debe sujetarse a lo establecido en la Ley 1581 de 2012, en el Decreto 1074 de 2015 y en las demás disposiciones que desarrollen lo relacionado con datos personales.

- **Principio de Finalidad**: El tratamiento realizado por el responsable y/o encargados obedece 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 releve el consentimiento.

- **Principio de Veracidad o Calidad:** Establece que 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 al 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.

- **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 presente ley y la Constitución.

  En este sentido, el tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en las disposiciones vigentes. Los datos personales salvo información pública no podrán estar disponibles en internet u otros medios de divulgación o comunicaciones masivas, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los titulares o terceros autorizados conforme a las normas vigentes.

- **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, perdida, consulta, uso o acceso no autorizado o fraudulento.

- **Principio de Confidencialidad**: Todas las personas que intervengan en el tratamiento de los 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 corresponde al desarrollo de las actividades autorizadas en la ley y en los términos de esta.

- **Principio de temporalidad:** Los datos personales se conservarán únicamente por el tiempo razonable y necesario para cumplir las finalidades que justificaron el tratamiento, atendiendo a las disposiciones aplicables a la materia de que se trate y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información. Los datos serán conservados cuando ello sea necesario para el cumplimiento de una obligación legal o contractual. Una vez cumplida la finalidad del tratamiento y los términos establecidos anteriormente, se procederá a la supresión de los datos.

- **Interpretación integral de los derechos constitucionales:** Los derechos se interpretarán en armonía y en un plano de equilibrio con el derecho a la información previsto en el artículo 20 de la Constitución y con los derechos constitucionales aplicables.

- **Principio de Necesidad:** Los datos personales tratados deben ser los estrictamente necesarios para el cumplimiento de las finalidades perseguidas con la base de datos.

- **Principio de Responsabilidad Demostrada (*Accountability*)**: Obliga al responsable del tratamiento a implementar y documentar políticas, procedimientos y mecanismos que acrediten el cumplimiento efectivo de las obligaciones legales en materia de protección de datos. Bajo este principio, no basta con aplicar las normas; es necesario conservar evidencia de las acciones realizadas (auditorías, registros de consentimiento, evaluaciones de riesgo, capacitaciones, etc.) para demostrar ante las autoridades y los titulares que se mantiene un manejo adecuado y transparente de la información personal.

6.1 Tratamiento justo, lícito y transparente

La legislación aplicable en materia de protección de datos en Colombia, incluido el GDPR en los casos en que este aplique de acuerdo a los datos tratados, no impide el tratamiento de datos personales, sino que garantiza que se traten de forma leal y sin menoscabo de los derechos de las personas.

Para ser justos, los ***datos personales*** deben tratarse con una base jurídica adecuada.

Por ejemplo:

- El sujeto de los datos ha dado su consentimiento previo y expreso o mediante actos inequivocos al tratamiento para uno o varios fines específicos;
- El tratamiento es necesario para ejecutar un contrato con el sujeto de los datos (o para tomar medidas a petición suya antes de celebrar un contrato);
- El tratamiento es necesario para cumplir nuestras obligaciones legales; o
- El tratamiento es necesario para nuestros intereses legítimos o los de una parte a la que se comunican los datos (a menos que prevalezcan los intereses del sujeto de los datos).

Cuando se traten **datos personales sensibles**, deberá aplicarse también al menos una base jurídica adicional. Por ejemplo:

- El sujeto de los datos ha consentido explícitamente o por conductas inequívocas el tratamiento para uno o varios fines específicos;
- El tratamiento es necesario para proteger la vida del sujeto de los datos (o de otra persona) intereses si el sujeto de los datos está física o jurídicamente incapacitado para dar su consentimiento; o
- El tratamiento se refiere a datos personales sensibles obviamente hechos públicos por el sujeto de los datos.

6.2 Tratamiento con fines limitados (finalidades del tratamiento)

Los datos personales que tratamos pueden incluir datos recibidos:

- Directamente de particulares (por ejemplo, cuando rellenan formularios o mantienen correspondencia con nosotros por correo, teléfono, correo electrónico u otros medios); y
- De otras fuentes (por ejemplo, socios comerciales, subcontratistas, agencias de referencia de crédito y otros).

Sólo trataremos los datos personales para los fines específicos establecidos en nuestra Política, o para cualquier otro fin específicamente permitido por la legislación aplicable en materia de protección de datos.

En concordancia, el tratamiento de los datos personales realizado por parte de **CALDIC** tiene como finalidad general permitir el adecuado desarrollo de su actividad empresarial y garantizar el cumplimiento de sus obligaciones legales, principalmente en los ámbitos contable, tributario, legal, comercial y/o laboral.

La información correspondiente a nuestros clientes, proveedores, socios y empleados, tanto presentes como anteriores, será administrada y protegida con el propósito de facilitar, fomentar, permitir o preservar relaciones de carácter comercial, civil y laboral, según aplique. Asimismo, se utilizará para cumplir con las obligaciones derivadas de los contratos y relaciones comerciales y laborales suscritas.

Las finalidades específicas del tratamiento de datos serán descritos en la presente politica y/o en anexos de la presente política y/o serán comunicados a las personas al momento de recopilar su información, garantizando su autorización conforme a la legislación colombiana.

Los datos suministrados por nuestros empleados serán utilizados con la finalidad de llevar a cabo procesos de selección para contratación interna, fortalecer sus competencias mediante cursos, capacitaciones, talleres, entre otros, e integrarlos en programas de bienestar y planes de beneficios, además de proporcionar referencias laborales, entre otros fines.

6.3 Autorización del titular de los datos

La autorización del titular podrá constar en un documento físico, electrónico, grabación magnetofónica, mensaje de texto o de datos, o en cualquier otro formato que permita garantizar su posterior consulta, o mediante un mecanismo técnico o tecnológico idóneo que permita concluir de manera inequívoca que, de no haberse surtido una conducta del titular, los datos nunca hubieren sido capturados y almacenados en la base de datos. La autorización será expedida por nosotros, y será puesta a disposición del titular, junto con el Aviso de Privacidad el cual podrá ser consultado de igual forma por el titular en la página web https://www.caldic.com/es-co.

6.4 Casos en que no es necesaria la autorización

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

a) Información requerida por la Entidad, en ejercicio de sus funciones legales o por orden judicial.
b) Datos de naturaleza pública.
c) Casos de urgencia médica o sanitaria.
d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.

e) 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 las Leyes 1581 de 2012, 1266 de 2008 y demás normas concordantes y vigentes.

6.5 Deber de informar al titular

Al momento de solicitar al Titular la autorización, se deberá informar a este de manera clara y expresa lo siguiente:

a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad de este.
b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes.
c) Los derechos que le asisten como Titular.
d) La identificación, dirección física o electrónica y teléfono del responsable del Tratamiento.

Nosotros como responsable del Tratamiento, conservaremos prueba del cumplimiento de lo previsto en el presente numeral y, cuando el Titular lo solicite, entregarle copia de esta.

6.6 Calidad de Datos

El dato personal objeto de tratamiento deberá ser veraz, completo, preciso, actualizado, verificable y claro. En caso de contar con datos personales que sean parciales, incompletos, fragmentados o que puedan inducir a error, nos abstendremos de realizar su tratamiento o procederemos a solicitar al Titular la actualización o corrección de la información.

Adicionalmente de acuerdo con las políticas de datos del grupo, los datos objeto del tratamiento deben cumplir con los siguientes requisitos, por lo tanto, estos deben ser:

- Adecuados
- Relevantes
- No excesivos
- Precisos
- Retención

A continuación, se explica el significado de cada uno de estos términos y cómo cumplimos estos requisitos en **CALDIC**:

Adecuación, Relevancia y No Excesivo

Sólo recopilaremos datos personales que sean adecuados, pertinentes y no excesivos y que sean necesarios para los fines específicos mencionados a las personas a las que se refieren los datos. Aplicamos un enfoque claro de "necesidad de conocer", lo que significa que los datos personales no circulan ni son accesibles de forma generalizada.

Precisión

Nos aseguraremos de que los datos personales que tenemos son exactos y se mantienen actualizados. Comprobaremos la exactitud de los datos personales en el momento de su recogida y posteriormente a intervalos regulares, y tomaremos todas las medidas razonables para destruir o modificar de forma segura los datos inexactos o caducados.

Retención

No conservaremos los datos personales más del tiempo razonable y necesario para cumplir las finalidades que justificaron el tratamiento, o hasta que necesario para el cumplimiento de una obligación legal o contractual.

Tomaremos todas las medidas razonables para destruir de forma segura, o borrar de nuestros sistemas, todos los datos que ya no sean necesarios.

6.7 Grabación de imágenes y videos.

CALDIC., cuenta con un sistema de video vigilancia el cual está instalado en diferentes sitios al interior de las instalaciones y en las oficinas de la Empresa. En virtud de lo anterior, **CALDIC**., recolecta imágenes, entendidas también como datos personales según lo establecido en la Ley 1581 del 2012 y el Decreto 1074 de 2015, a través de sus cámaras de vigilancia tanto de sus trabajadores como de sus clientes, proveedores y en general de los visitantes que ingresan a sus diferentes instalaciones.

Los datos personales son almacenados en una base de datos la cual es calificada por la Empresa como de reserva, y cuya información no será revelada a ningún tercero salvo en los casos en que medie autorización expresa del titular o por una orden o solicitud formal de una autoridad competente.

Las finalidades para las cuales son utilizados los datos personales contenidos en las cámaras de vigilancia de **CALDIC**, serán para efectos de garantizar la seguridad de sus trabajadores, visitantes y cualquier tercero que ingrese a sus instalaciones, así como para garantizar la seguridad de los bienes e instalaciones, garantizar la seguridad en los ambientes laborales, permitir ambientes de trabajo adecuados para el desarrollo seguro de actividades laborales de la Compañía, controlar el ingreso, permanencia y salida empleados y visitantes en las instalaciones de la compañía, control subordinante fines disciplinarios, sancionatorios, de gestión del rendimiento o investigaciones penales.

De conformidad con el objeto social de **CALDIC**, la compañía, directa o indirectamente, podrá realizar la grabación de imágenes, videos, voz, etc. de los usuarios, clientes, proveedores y demás terceros que se encuentren dentro de las locaciones.

Para efectos de dar cumplimiento al deber de información, **CALDIC**, como responsable del tratamiento de los datos personales de que trata el presente numeral, tiene implementados *avisos de privacidad* dentro de sus instalaciones, especialmente en las zonas en donde se encuentran situadas las cámaras grabación y de vigilancia, para efectos de que los titulares de los datos personales puedan conocer sus derechos y conocer el alcance del tratamiento.

Con el ingreso a nuestras instalaciones, el titular de los datos personales acepta inequívocamente el tratamiento de sus datos, sin embargo, tiene derecho a conocer, corregir, actualizar, rectificar o suprimir los datos personales tratados por nuestra compañía.

El periodo de conservación de las grabaciones no será indefinido; en condiciones normales se mantendrán por un plazo máximo de 60 días. Únicamente en casos excepcionales, por ejemplo, procesos de investigación interna, control subordinante, fines disciplinarios, sancionatorios, de gestión del rendimiento o investigaciones judiciales o administrativas se podrá extender su retención hasta que concluya el proceso correspondiente.

Los titulares de las grabaciones podrán ejercer su derecho de acceso a los datos que les conciernen, solicitando copia de las mismas ante el responsable del tratamiento. Esta solicitud será atendida de manera oportuna y gratuita, siempre y cuando su ejercicio no comprometa derechos de terceros ni ponga en riesgo la seguridad física, operativa o reputacional de **CALDIC**. En caso de que el acceso solicitado afecte información sensible de otras personas o procesos internos críticos, el responsable podrá denegar total o parcialmente la entrega, fundamentando su decisión y ofreciendo, cuando sea posible, alternativas que garanticen la protección de todos los involucrados.

6.8 Registro de llamadas telefónicas:

CALDIC, puede comunicar que las llamadas telefónicas entrantes y salientes podrán ser grabadas y monitoreadas por motivos de calidad del servicio, seguridad, control subordinante.

Los registros también servirán como evidencia de cualquier solicitud que se realice a La empresa. Esta información será tratada de manera interna, garantizando el cumplimiento de las premisas de privacidad y seguridad de la información.

Estas grabaciones se conservarán por un periodo máximo de 60 días, salvo en casos excepcionales de investigación interna o requerimientos judiciales, con el fin de garantizar la disponibilidad oportuna de la información necesaria, cumplir con obligaciones legales y preservar la privacidad.

6.9 Transferencia y transmisión de Datos Personales

Los datos personales y sensibles que recopilamos podrán ser transferidos o transmitidos a terceros con quienes se tenga relación legal, comercial y operativa que le provean de servicios necesarios para su debida operación, o de conformidad con las funciones establecidas a su cargo en las leyes.

En dichos supuestos, se adoptarán las medidas necesarias para que las personas que tengan acceso a sus datos personales cumplan con la presente Política y con los principios de protección de datos personales y obligaciones establecidas en la Ley.

En todo caso, cuando se realice la transmisión de los datos a uno o varios encargados ubicados dentro o fuera del territorio de la República de Colombia, se establecerán cláusulas contractuales o se celebrarán contratos de transmisión de datos personales en el que indicará: (i) los alcances del tratamiento, (ii) las actividades que el encargado realizará por cuenta del responsable para el tratamiento de los datos personales y, (iii) las obligaciones del Encargado para con el titular y el responsable. De igual forma se procederá cuando realice la transferencia de datos a uno o varios responsables ubicados dentro o fuera del territorio de la República de Colombia.

Mediante dicho acuerdo o clausulas el Encargado se comprometerá a dar aplicación a las obligaciones del

responsable bajo la política de Tratamiento de la información fijada por este y a realizar el Tratamiento de datos de acuerdo con la finalidad que los Titulares hayan autorizado y con las leyes aplicables vigentes. Además de las obligaciones que impongan normas aplicables dentro del citado contrato, deberán incluirse las siguientes obligaciones en cabeza del respectivo encargado:

- Dar Tratamiento, a nombre del responsable, a los datos personales conforme a los principios que los tutelan.
- Salvaguardar la seguridad de las bases de datos en los que se contengan datos personales.
- Guardar confidencialidad respecto del tratamiento de los datos personales. En caso de transferencia se dará cumplimiento a las obligaciones estipuladas en la Ley 1581 de 2012 y normas reglamentarias.

Los datos personales y sensibles que recopilamos pueden transferirse y almacenarse en destinos fuera de la región en la que se originaron/recopilaron, siempre que cumplamos una de una serie de condiciones. Entre ellas se incluyen, por ejemplo, condiciones que:

- El país u organización internacional al que se transfieren los datos personales garantiza **una protección adecuada** de los datos objeto de la transferencia o transmisión de acuerdo con el marco normativo colombiano;
- Las personas han **consentido explícitamente** el traslado mediante autorización de tratamiento de datos;
- La transferencia **es necesaria** por uno de los motivos relacionados nuestra operatividad, para lo cual se deberán acatar las directrices legales establecidas en la legislación colombiana en materia de protección de datos, incluida la ejecución de un contrato entre nosotros y las personas en cuestión, o para proteger los intereses vitales de las personas, de acuerdo con lo enunciado anteriormente, siempre que se cumpla con lo dispuesto en el artículo 26 de la Ley 1581 de 2012;
- la transferencia es necesaria por **razones importantes de interés público** o para el establecimiento, ejercicio o defensa de reclamaciones legales;
- la transferencia esté autorizada por la autoridad competente (declaracion de conformidad).

6.10 Garantías generales y administrativas

Hemos desarrollado, implantado y mantenemos salvaguardas administrativas y físicas razonables de conformidad con la legislación y las normas aplicables para proteger la seguridad, confidencialidad, integridad y disponibilidad de los datos personales que poseemos.

Las garantías deberán ser adecuadas a nuestro tamaño, alcance y actividad, a nuestros recursos disponibles y a la cantidad de datos personales que conservamos o mantenemos en nombre de terceros, reconociendo al mismo tiempo la necesidad de proteger tanto la información de nuestros empleados, proveedores, clientes y/o cualquier tercero.

Documentaremos nuestras garantías administrativas y físicas en nuestras políticas y procedimientos de seguridad de la información.

Nuestras garantías administrativas incluyen, como mínimo:

- Designar a uno o varios miembros del personal o área encargada para coordinar el programa de

seguridad de la información;

- Limitar la cantidad de datos personales recogidos a la razonablemente necesaria para cumplir nuestros fines empresariales legítimos, o para cumplir la legislación colombiana;
- Limitar el acceso a los registros de datos personales a aquellas personas que razonablemente deban conocer dicha información para cumplir nuestro legítimo propósito comercial o permitirnos cumplir la legislación colombiana;
- Identificar los riesgos internos y externos razonablemente previsibles, y evaluar si las garantías existentes controlan adecuadamente dichos riesgos;
- Formación del personal en prácticas y procedimientos del programa de seguridad, con supervisión de la dirección;
- Seleccionar proveedores de servicios (incluidos, entre otros, los encargados del tratamiento de datos) capaces de mantener las garantías adecuadas, y exigirles contractualmente que lo hagan de acuerdo con la presente politica, y;
- Ajustar nuestro programa de seguridad de la información a la luz de los cambios empresariales o de nuevas circunstancias.

6.10.1 Garantías físicas

Nuestras garantías físicas deberán, como mínimo, prever:

- Definir y aplicar medidas razonables de seguridad física para proteger las zonas en las que se pueda acceder a los datos personales, lo que incluye restringir razonablemente el acceso físico y almacenar los registros de datos personales en instalaciones, zonas o contenedores cerrados con llave;
- Prevenir, detectar y responder a intrusiones o accesos no autorizados a datos personales, incluso durante o después de su recogida, transporte o eliminación;
- Eliminar o destruir de forma segura los datos personales, ya sea en papel o en formato electrónico, cuando ya no deban conservarse de conformidad con la legislación aplicable o las normas aceptadas.

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

7.1 Deberes de GTM Colombia S.A. como responsable del tratamiento.

Como responsable del Tratamiento, nuestra compañía deberá cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la ley y en otras que rijan su actividad:

- Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- Conservar, en las condiciones previstas en la ley, copia de la respectiva autorización otorgada por el Titular o prueba de ella.
- Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
- Conservar la información bajo las condiciones de seguridad razonables para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- 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 este se mantenga actualizada.
- Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.
- Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la ley.
- Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
- Tramitar las consultas y reclamos formulados en los términos señalados en la ley.
- Adoptar procedimientos específicos para garantizar el adecuado cumplimiento de la ley y en especial, para la atención de consultas y reclamos.
- 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.

- Informar a solicitud del Titular sobre el uso de sus datos.
- n. 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.

7.2 Deberes de los encargados del tratamiento

Los Encargados del Tratamiento, y en el evento en el cual **GTM COLOMBIA S.A.**, actúe como encargada, deberán cumplir los deberes del responsable que le sean aplicables y, las siguientes:

- Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles siguientes contados a partir de su recibo.
- Permitir el acceso únicamente a las personas autorizadas por el Titular o facultadas por la ley para dicho efecto, la información únicamente a las personas autorizadas por la Ley para ello.

8. Derechos de los titulares de los datos

Trataremos todos los datos personales en consonancia con los derechos de las personas, en la medida exigida por la legislación colombiana y de conformidad con la misma.

Los usuarios de datos deben ponerse en contacto con el Departamento Jurídico y de Cumplimiento si reciben solicitudes de particulares en relación con tales derechos.

De acuerdo con lo anterior los titulares de datos personales gozan de los siguientes derechos:

- Conocer, actualizar y rectificar sus datos personales frente a los responsables del Tratamiento o Encargados del Tratamiento.
- 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 1581 de 2012;
- Ser informado por el responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que les ha dado a sus datos personales;
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la ley y las demás normas que la modifiquen, adicionen o complementen;
- Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión no procederá cuando los datos deban ser conservados para el cumplimiento de una obligación legal o contractual;
- Acceder en forma gratuita a los datos personales que hayan sido objeto de Tratamiento.
- Los demás derechos que se encuentren contenidos en la normatividad vigente que regula la materia.

En ejercicio de los derechos anteriormente listados podrá realizar las consultas que resulten pertinentes y realizar los reclamos que entienda necesarios de cara a garantizar el respeto de los mismos.

Adicionalmente de acuerdo con las políticas del grupo, los titulares gozarán de los siguientes derechos:

- Salvo determinadas excepciones, borraremos los datos personales de las personas físicas que lo

soliciten sin dilación indebida en determinadas circunstancias (por ejemplo, si sus datos personales ya no son necesarios para los fines para los que se recogieron).

- Restringiremos el tratamiento de los datos personales de las personas físicas en determinadas circunstancias (por ejemplo, si consideran que sus datos personales que obran en nuestro poder son inexactos), si así lo solicitan.
- Respetaremos los derechos de las personas a recibir los datos personales que nos hayan facilitado en un formato estructurado, de uso común y lectura mecánica, y a facilitar dichos datos personales a otro responsable del tratamiento sin que nosotros se lo impidamos en determinadas circunstancias.
- Respetaremos el derecho de las personas a oponerse al tratamiento de sus datos personales en determinadas circunstancias.
- Respetaremos los derechos de las personas en relación con el uso de sus datos personales para la comercialización directa.
- Respetaremos el derecho de las personas (salvo determinadas excepciones) a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos personales, incluida la elaboración de perfiles, especialmente cuando ello tenga efectos jurídicos u otros efectos significativos sobre ellas.
- Garantizaremos que las personas siempre puedan obtener una revisión por parte de nuestro personal de cualquier decisión automatizada, puedan expresar sus opiniones e impugnar dichas decisiones.

9. Ejercicio de derechos por los titulares de los datos

9.1 Área responsable de la atención a consultas, solicitudes, quejas y reclamaciones

Las consultas, solicitudes, quejas y reclamaciones formulados por los titulares de Datos Personales bajo Tratamiento de **CALDIC** para ejercer sus derechos a conocer, actualizar, rectificar y suprimir datos, o revocar la autorización deberán ser dirigidas a:

- Correo electrónico: privacy_col@caldic.com

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

9.2 Procedimiento de consultas

Garantizamos 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 de Tratamiento de Datos Personales.

9.3 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.

9.4 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.

9.5 Procedimiento de reclamos

Derechos Garantizados mediante el procedimiento de reclamos:

- **Corrección o Actualización:** garantizamos 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 de Tratamiento de Datos Personales para que sea procedente la solicitud de Corrección o Actualización.

- **Revocatoria de la autorización o Supresión de los datos Personales**: Garantizamos 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 de Tratamiento de Datos Personales.

  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 de tratamiento de datos personales.

9.6 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.

9.7 Prórroga del plazo de respuesta

Cuando no fuere posible atender el reclamo dentro de dicho término, se informaremos 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.

9.8 Reclamaciones sin cumplimiento de requisitos legales

En caso de que la reclamación se presente sin el cumplimiento de los anteriores requisitos legales, solicitaremos 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.

9.9 Desistimiento del reclamo

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

10. Seguridad de los datos

Mantenemos la seguridad de los datos protegiendo la confidencialidad, integridad y disponibilidad de los datos personales, definidos de la siguiente manera:

- Confidencialidad significa que sólo pueden acceder a los datos las personas autorizadas a utilizarlos;
- Integridad significa que los datos personales deben ser exactos y adecuados a los fines para los que se tratan;
- Disponibilidad significa que los usuarios autorizados deben poder acceder a los datos si los necesitan para fines autorizados.

Entre otras cosas, nuestros procedimientos de seguridad incluyen:

- **Controles de entrada**
  Se debe informar de cualquier extraño visto en las zonas de entrada controlada.

- **Escritorios y armarios seguros con cerradura**
  Los escritorios y armarios deben mantenerse cerrados con llave casi contengan información confidencial de cualquier tipo (la información personal siempre se considera confidencial).

- **Métodos de eliminación**
  Los documentos en papel deben triturarse y los dispositivos de almacenamiento digital deben destruirse físicamente cuando ya no se necesiten.

- **Equipos**
  Los usuarios de datos deben asegurarse de que los monitores individuales no muestren información confidencial a los transeúntes y de que se desconecten de sus PC cuando los dejen desatendidos.

- **Archivos en papel**
  Los archivos en papel y otros registros de datos personales deben guardarse de forma segura.

Protección por contraseña
Los datos personales conservados en ordenadores y sistemas informáticos deben protegerse mediante el uso de contraseñas seguras que, en la medida de lo posible, obliguen a cambiar periódicamente. No debería ser posible comprometer fácilmente contraseñas individuales.

GTM COLOMBIA S.A. ha designado un departamento de TI que es responsable de la seguridad de los datos. El departamento de TI ha publicado sus propias políticas (más detalladas) en torno a la seguridad de los datos.

El departamento de TI es responsable de aplicar, coordinar y mantener las medidas de seguridad de los datos. Entre estas medidas figuran las siguientes:

- Evaluar los riesgos internos y externos para los datos personales y mantener la documentación correspondiente, incluidos los informes de evaluación de riesgos y los planes de corrección;
- Coordinar el desarrollo, distribución y mantenimiento de las políticas y procedimientos de seguridad de la información;
- Coordinar el diseño de garantías administrativas, técnicas y físicas razonables y adecuadas para proteger los datos personales;
- Supervisar a los empleados, miembros del consejo de administración, proveedores de servicios y contratistas independientes que acceden a los datos personales o los conservan en nuestro nombre;
- Monitorear y probar la implementación y la eficacia de la seguridad de datos de manera continua
- Definir y gestionar los procedimientos de respuesta a incidentes, y
- Establecer y gestionar políticas y procedimientos de aplicación para la seguridad de los datos.

11. Retención

Los datos personales serán tratados por el tiempo razonable y necesario para cumplir las finalidades que justificaron el tratamiento, o hasta que necesario para el cumplimiento de una obligación legal o contractual.

Todos nuestros empleados y contratistas deben tener en cuenta la siguiente excepción general a cualquier calendario de destrucción establecido:

- Si usted cree, o el Departamento Jurídico y de Cumplimiento le informa, que nuestros registros de datos personales son relevantes para un litigio en curso, un litigio potencial, una investigación gubernamental, una auditoría u otro acontecimiento, deberá conservar y no borrar, eliminar, destruir o modificar dichos registros, incluidos los correos electrónicos, hasta que el Departamento de Cumplimiento determine que dichos registros ya no son necesarios;
- Esta excepción sustituye a cualquier calendario de destrucción de dichos registros establecido con anterioridad o posteriormente; y
- Si cree que puede aplicarse esta excepción, o tiene alguna pregunta, póngase en contacto con el departamento Jurídico y de Cumplimiento

También se le puede pedir que suspenda cualquier procedimiento rutinario de eliminación de documentos de datos personales en relación con otros tipos de acontecimientos, como la fusión de **GTM COLOMBIA S.A.** con otra organización o la sustitución de nuestros sistemas de tecnología de la información.

Cada jefe de departamento es responsable del proceso continuo de identificación de los registros de datos personales que han cumplido el periodo de conservación exigido y de la supervisión de su destrucción.

La destrucción de registros físicos o manuales de datos personales debe realizarse mediante trituración, mientras que la destrucción de registros electrónicos debe coordinarse con el Departamento de Informática.

La destrucción de registros de datos personales debe cesar inmediatamente tras la notificación del Departamento Jurídico y de Cumplimiento de que podemos estar implicados en un pleito o en una

investigación oficial. La destrucción podrá reanudarse previa notificación del Departamento Jurídico y de Cumplimiento.

12. Incidentes de seguridad

Un "***incidente de seguridad***" es cualquier violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la difusión o el acceso no autorizados, de datos personales transmitidos, conservados o tratados de otra forma por **CALDIC**.

Los incidentes de seguridad relacionados con el tratamiento de datos personales son cada vez más frecuentes y pueden producirse de diversas maneras.

Algunos ejemplos no exhaustivos de cómo pueden producirse incidentes de seguridad relacionados con el tratamiento de datos personales son:

- Pérdida o robo de documentos que contengan datos personales o de equipos en los que se almacenen datos personales (por ejemplo, documentos en papel, ordenadores portátiles, teléfonos inteligentes o unidades USB que contengan datos personales y que se hayan dejado accidentalmente en lugares públicos, o que hayan sido robados en nuestros locales);
- Acceso o uso no autorizado de nuestros datos (por ejemplo, si un miembro del personal accede a datos personales cuando no está autorizado para ello, o que no son necesarios para su función concreta, o si se hace un uso no autorizado de la contraseña o tarjeta de acceso de un miembro del personal, o si se envían datos personales a un tercero sin autorización);
- Error humano, (por ejemplo, si se enviaron datos personales a un destinatario no autorizado o incorrecto por correo electrónico, carta o fax, o se perdió una tarjeta llave de la oficina que permitió a una persona no autorizada para acceder a zonas seguras de nuestras instalaciones en las que los datos personales eran accesibles o se podían ver);
- Destrucción insegura de documentos o soportes que contengan datos personales (por ejemplo, si para la eliminación de documentos se utilizan contenedores no seguros en lugar de contenedores seguros para la trituración/eliminación y destrucción de documentos confidenciales);
- Acontecimientos que escapen a nuestro control (por ejemplo, si se produce un incendio o una inundación que provoque el fallo de los equipos o la destrucción de los datos personales);
- Ataques de piratas informáticos que den lugar a que terceros obtengan acceso no autorizado a nuestros sistemas informáticos y datos personales;
- Delitos de "phishing" en los que la información se obtiene de nosotros mediante engaño, (por ejemplo, si un tercero se hace pasar por un miembro del Personal o un Cliente para obtener acceso no autorizado a datos personales o se envía un correo electrónico de "phishing" al Personal que conduce a una infección por malware de nuestros Sistemas de TI);
- Fallo de los equipos (por ejemplo, si fallan nuestros servidores, lo que provoca la pérdida o corrupción de datos personales, o si fallan nuestros cortafuegos, lo que permite a terceros no autorizados acceder a nuestros sistemas).
- El secuestro de datos mediante ataques de ransomware supone que un atacante introduce software malicioso que cifra la información crítica de la organización, impidiendo el acceso legítimo hasta que se pague un rescate. Este tipo de incidente no solo paraliza operaciones

y pone en riesgo la disponibilidad de los datos personales, sino que puede derivar en su divulgación pública si no se accede a las exigencias del atacante, lo que vulnera gravemente la confidencialidad y la integridad de la información tratada.

- Vulnerabilidades de configuración, se producen cuando sistemas, aplicaciones o servicios en la nube quedan expuestos por ajustes erróneos (por ejemplo, permisos abiertos en repositorios o buckets sin protecciones adecuadas), lo que permite a usuarios no autorizados acceder, modificar o extraer datos personales. Estos errores de configuración pueden deberse a políticas de acceso demasiado laxas, credenciales predeterminadas sin cambiar o falta de cifrado en tránsito y reposo, y comprometen la confidencialidad y la integridad de la información al facilitar el acceso no controlado a los datos.
- Brechas de proveedores o terceros aquellos incidentes de seguridad originados en socios, proveedores o servicios subcontratados que, teniendo acceso a datos personales por cuenta de CALDIC, sufran vulneraciones o fallos en sus controles y deriven en la divulgación, alteración o pérdida de la información. Para mitigarlas, se incluirán cláusulas de seguridad y notificación en los contratos, se evaluará periódicamente el nivel de protección de los terceros y se exigirá la aplicación de estándares equivalentes a los de GTM en materia de confidencialidad, integridad y disponibilidad.
- Errores en actualizaciones o parches de seguridad aquellos fallos derivados de la aplicación incorrecta, incompleta o tardía de actualizaciones críticas en sistemas, aplicaciones o dispositivos, que dejen vulnerabilidades sin corregir y permitan a atacantes comprometer la confidencialidad, integridad o disponibilidad de los datos personales. Para evitarlos, mantendremos un programa de gestión de parches que incluya fases de prueba previas, aprobación formal, despliegue coordinado y registro de cada actualización, así como revisiones periódicas para garantizar que todos los componentes cuenten con las versiones más seguras.

12.1. Riesgos de incidentes de seguridad relacionados con el tratamiento de datos personales

Los incidentes de seguridad relacionados con el tratamiento de datos personales pueden tener una serie de consecuencias adversas, tanto para los titulares de los datos afectados por la violación como para **CALDIC.**

Los incidentes de seguridad relacionados con el tratamiento de datos personales pueden provocar angustia emocional y/o diversos tipos de daños físicos y/o financieros a los titulares, entre ellos:

- Pérdida de control sobre sus datos personales (por ejemplo, información sobre la vida privada de una persona que se conozcan, como la limitación de sus derechos a la intimidad;
- Discriminación;
- Robo de identidad, fraude y/o pérdidas financieras;
- Daños a la reputación;
- Otras desventajas económicas o sociales para el sujeto de los datos.

Los incidentes de seguridad relacionados con el tratamiento de datos personales también pueden acarrear una serie de consecuencias adversas para **CALDIC**, entre las que se incluyen:

- Pérdida de la confianza de nuestros empleados, Clientes y/o proveedores;
- medidas coercitivas, incluidas importantes sanciones económicas;

- Particulares que emprendan acciones contra **CALDIC** y reclamen indemnizaciones (incluso a través de procedimientos de tipo acción de grupo); y
- Importantes daños a la reputación y publicidad negativa.

Si se produce un incidente de seguridad relacionado con datos personales, estamos obligados a notificarlo a la Superintendencia de Industria y Comercio como autoridad de protección de datos pertinente dentro del plazo establecidos por en el Título Quinto de la Circular Única de la Superintendencia de Industria y Comercio, es decir, 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, estemos o no obligados a registrar bases de datos en el RNBD.

12.2. Qué hacer si descubre una brecha de datos

Si descubre, tiene conocimiento o sospecha de que se está produciendo o se ha producido un incidente de seguridad relacionado con el tratamiento de datos personales debe proceder de la siguiente manera:

- Póngase **siempre** en contacto de **inmediato** con el departamento de TI y con el departamento Jurídico y de Cumplimiento, incluso si no está seguro de que se haya producido una violación o de si la violación afecta o no a datos personales; y
- Coopere plenamente con cualquier investigación o respuesta a cualquier infracción confirmada o sospechada y cumplir con cualquier instrucción del departamento de TI y Jurídico y de Cumplimiento lo antes posible para garantizar que cumplimos con nuestras obligaciones dentro de los plazos requeridos.

Los departamentos de TI y Jurídico y de Cumplimiento colaboran estrechamente en este ámbito ya que son responsables de:

- Reportar los incidentes de seguridad de GTM Colombia relacionados con el tratamiento de datos personales ante las autoridades competentes, esto es a la autoridad de control (SIC), a las personas afectadas por la violación y/o a terceros;
- Decidir si se está produciendo o se ha producido una infracción en casos poco claros;
- Gestionar cualquier violación o sospecha de violación de los datos personales y ponerse en contacto con el personal pertinente y otros terceros para obtener información de ellos;
- Investigar, contener y recuperar, evaluar los riesgos de, evaluar, responder a y documentar la violación pertinente, y a menos que esté específicamente autorizado para ello por el departamento de TI o el departamento Legal y de Cumplimiento.

No debe hacerlo bajo ninguna circunstancia:

- Emprender cualquiera de las acciones de las que es responsable el departamento de TI y Cumplimiento, según lo expuesto anteriormente; o
- Revelar de otro modo detalles de (incluida la existencia o sospecha de existencia de) cualquier incidente de seguridad relacionado con el tratamiento de datos personales personales a cualquier otra persona o tercero (incluido nuestro otro personal) que no sea el departamento de TI y Jurídico y de Cumplimiento.

Para más información y orientación sobre incidentes de seguridad relacionados con el tratamiento de datos personales y/o nuestras medidas de seguridad de datos personales, póngase en contacto con el area

encargada de proteccion de datos de CALDIC o al departamento de TI o con el departamento Jurídico y de Cumplimiento.

13. Evaluación de riesgos

CALDIC realizará evaluaciones de riesgos periódicas y documentadas. La evaluación de riesgos deberá:

- Identificar los riesgos internos y externos razonablemente previsibles para la seguridad, confidencialidad, integridad o disponibilidad de cualquier registro electrónico, en papel o de otro tipo de datos personales;
- Evaluar la probabilidad y los daños potenciales que podrían derivarse de tales riesgos, teniendo en cuenta la sensibilidad de los datos personales;
- Evaluar la adecuación de las políticas, procedimientos, sistemas y garantías pertinentes establecidos para controlar dichos riesgos, en ámbitos que incluyen, por ejemplo:

    a) Formación y gestión del personal y las partes interesadas,
    b) Cumplimiento de esta política y de las políticas y procedimientos conexos por parte del personal y las partes interesadas,
    c) sistemas de información, incluida la adquisición, el diseño, la aplicación, las operaciones y el mantenimiento de redes, ordenadores y programas informáticos, así como el tratamiento, almacenamiento, transmisión, conservación y eliminación de datos, y
    d) nuestra capacidad para prevenir, detectar y responder a ataques, intrusiones y otros incidentes de seguridad o fallos del sistema.

Si utilizamos procesadores de datos, o cualquier otro tercero, que tengan acceso a cualquier dato personal que recopilemos y/o utilicemos, seleccionamos y contratamos procesadores de datos capaces de mantener la privacidad, seguridad, integridad y confidencialidad de cualquier dato personal al que puedan acceder.

También exigimos a todos los procesadores de datos, mediante contratos escritos adecuados, que apliquen salvaguardas razonables para proteger los datos personales y que cumplan (y garanticen que nosotros cumplimos) todas las leyes de protección de datos aplicables y todas las disposiciones aplicables de esta Política y de nuestras Políticas de Seguridad de Datos Personales y de Vulneración de Datos Personales.

Todos los terceros pertinentes (por ejemplo, todos los contratistas, agentes, personas o entidades que trabajen para nosotros) deben asegurarse de que ellos y todo su personal que procese datos personales en nuestro nombre conozcan la legislación aplicable en materia de protección de datos.

Si los usuarios de datos desean designar o compartir datos personales con procesadores de datos, deben tener un Acuerdo de Procesamiento de Datos firmado. **CALDIC** dispone de un Acuerdo Normalizado de Tratamiento de Datos que puede utilizarse para estos fines. Si desea una copia del Acuerdo de Tratamiento de Datos, póngase en contacto con el Departamento Jurídico y de Cumplimiento.

14. Monitorización

CALDIC comprobará y supervisará periódicamente la aplicación y eficacia de esta Política y de nuestros procedimientos de seguridad de la información para garantizar que funcionan de un modo razonablemente calculado para impedir el acceso o uso no autorizados de datos personales.

La supervisión, de conformidad con la legislación y la normativa aplicables, abarcará el acceso de todo el personal y los proveedores de servicios, incluidos los encargados del tratamiento de datos.

Abordaremos de forma razonable y adecuada las lagunas detectadas.

15. Cookies

Nuestros sitios web utilizan cookies y otras tecnologías de seguimiento (si usted está de acuerdo) cuando usted visita nuestros sitios web estas cookies se utilizan de varias maneras, por ejemplo, para distinguirle de otros usuarios de nuestros sitios web, para entender cómo está utilizando nuestros sitios web, para ayudarnos a ofrecerle una buena experiencia cuando navega por nuestros sitios web y para mejorar nuestros sitios web

Para obtener más información sobre las cookies que utilizamos y cómo las utilizamos, revise nuestra Política de cookies en nuestro sitio web https://www.caldic.com/es-co.

Propiedad del Documento

El Departamento Jurídico y de Cumplimiento asume la titularidad y responsabilidad de este documento, por tanto, garantiza que vela por su revisión oportuna y adecuada.

Anexo I:
Protección de Datos de los Empleados

Este Anexo (y cualquier otro documento al que se haga referencia en él) establece las bases sobre las que **CALDIC** procesará y utilizará cualquier dato personal sobre nuestros solicitantes de empleo y empleados que obtengamos de ellos, que ellos nos proporcionen o que obtengamos de terceros.

CALDIC cumplirá en todo momento con toda la normativa aplicable y ha establecido en esta Política y en otras políticas que tenemos, ciertas normas y directrices como punto de partida. Este anexo establece las prácticas relativas tratamiento de datos del personal/empleados y cómo CALDIC la tratará.

Candidatos, empleados, contratistas y proveedores

CALDIC puede (sólo si lo permite la normativa aplicable) recopilar, utilizar y en general realizar el tratamiento de diversos tipos de datos personales tanto de nuestros solicitantes de empleo como de nuestros empleados, incluidos los siguientes:

Candidatos

- Cuando realice consultas sobre ofertas de empleo, solicite puestos, recopilaremos su nombre y datos de contacto para poder facilitarle la información pertinente y estudiar sus solicitudes.
- También le pediremos que nos facilite una carta de presentación, su CV y cualquier otra documentación pertinente.
- También le pediremos que confirme si está autorizado a trabajar en el país que ha solicitado de forma permanente.
- Recopilaremos notas durante las entrevistas que pueda mantener con nosotros.
- Podemos recopilar y utilizar otros datos personales cuando mantenemos correspondencia con usted (ya sea por teléfono, correo electrónico u otros medios).
- Podemos recopilar cierta información personal cuando nos comunique problemas con nuestros sitios web.
- Cuando visite nuestros sitios web, recopilaremos determinada información técnica sobre usted y su visita (por ejemplo, el dominio de Internet desde el que accede a nuestros sitios web, su dirección de protocolo de Internet, su tipo y versión de navegador, su sistema operativo y plataforma, las fechas y horas en las que accede a nuestros sitios web, los sitios web o enlaces que utiliza para acceder a nuestros sitios web, la información de inicio de sesión, los detalles de los productos o servicios que ve o busca, la información relativa a su comportamiento al hacer clic, las páginas que visita, los destinos que solicita, las páginas por las que sale de nuestros sitios web y los localizadores uniformes de recursos completos, ("URL").
- Podemos recopilar datos sobre sus preferencias de marketing y sobre si desea o no recibir determinados mensajes de marketing de nuestra parte (por ejemplo, correos electrónicos de marketing y boletines informativos), así como sobre la obtención/retirada de dicho consentimiento.

Empleados y contratistas

También podemos recopilar y utilizar varios tipos adicionales de información personal sobre nuestros empleados y/o colaboradores en otras modalidades contractuales, exclusivamente, incluidos los siguientes:

- Recopilaremos fotografías, otras imágenes visuales y/o descripciones personales suyas, junto con datos sobre su fecha de nacimiento y edad.
- Registraremos datos sobre su estado civil, familia y datos de contacto en caso de emergencia (incluidos nombres, apellidos y números de teléfono de los familiares más próximos).
- Recopilaremos datos sobre las escuelas y centros de enseñanza superior a los que ha asistido, así como sobre sus cualificaciones y otros cursos de formación pertinentes.
- Recopilaremos datos sobre su empleo actual y anterior, así como referencias laborales.
- Mantendremos registros de administración del empleo con respecto a usted.
- Recopilaremos y mantendremos datos sobre sus exámenes médicos y seguimiento de estado de salud, de acuerdo con los requerimientos de salud ocupacional y recursos humanos.
- Mantendremos registros de su salario, prestaciones y datos financieros, número de la seguridad social u otro número de la seguridad social, datos de identificación fiscal, copias de su pasaporte, otros documentos de identificación emitidos por el Gobierno y datos bancarios o de la sociedad de crédito hipotecario e información sobre cuentas.
- Recopilamos parte de la información personal mencionada directamente de usted y otra parte de terceros (como centros educativos, antiguos empleadores y personas de referencia).

Datos personales que recopila CALDIC y base legal para su tratamiento

CALDIC necesitará la información personal mencionada anteriormente porque es relevante para celebrar determinados contratos, por ejemplo, contratos de trabajo y contratos en relación con los requisitos de pensiones y seguros de los empleados.

Pedimos a los empleados autorización para realizar el tratamiento de sus datos personales. El consentimiento es siempre voluntario. Sin embargo, si no da su consentimiento, es probable que no podamos cumplir algunos requisitos contractuales.

Recopilamos y utilizamos esta información personal según sea necesario para nuestros intereses legítimos a la hora de proporcionarle la información que solicite, considerarle para los puestos que solicite y celebrar contratos de trabajo y contratos relacionados con usted, si procede.

Si nos facilita información sobre terceros (por ejemplo, datos de contacto en caso de emergencia), le pedimos que confirme que ha obtenido el consentimiento de los terceros en cuestión para hacerlo.

Categorías especiales de información personal "sensible"

También podemos realizar el tratamiento de datos sensibles sobre nuestros empleados para administrar la relación laboral y cumplir con nuestras obligaciones legales en materia de empleo, incluidas las siguientes:

- Podemos recopilar datos sobre el origen racial o étnico.
- Podemos recabar datos sobre la afiliación sindical.
- Podemos recopilar datos durante la comprobación de antecedentes penales en relación con delitos, condenas y procedimientos y sentencias judiciales relacionados.

Recopilamos esta información directamente de usted y parte de ella de terceros, pero sólo con su consentimiento explícito. Dependiendo de su función, podemos solicitar un certificado de buena conducta a las autoridades gubernamentales locales y en general realizar estudios de seguridad y de antecedentes

ante las entidades correspondientes en el territorio colombiano y fuera de este.

Necesitamos las categorías especiales de información personal sobre usted para celebrar determinados contratos. Por ejemplo, necesitamos realizar comprobaciones de antecedentes en relación con los contratos para determinados puestos directivos.

Si no está dispuesto a dar su consentimiento, es probable que no se cumplan algunos de los requisitos contractuales pertinentes.

Recopilamos y utilizamos su información personal sensible sólo si tenemos su consentimiento explícito para utilizar esta información que nos permita administrar la relación laboral con usted. Si consiente el uso de su información personal sensible, puede retirar su consentimiento en cualquier momento, pero esto no afectará a la legalidad de cualquier uso anterior a la retirada de su consentimiento.

Finalidades del tratamiento de los datos personales de nuestros Colaboradores, Empleados y Candidatos

Recopilamos y utilizamos información personal y sensible sobre nuestros colaboradores, empleados y Candidatos para los siguientes fines:

- Fines de contratación y/o proceso de contratación;
- Mantener correspondencia y registrar cualquier comunicación;
- Realizar la evaluación de los candidatos a ser evaluados, con el propósito que CALDIC adelante según lo considere conveniente, en procesos de selección.
- Retomar o contactarlo nuevamente para procesos de contratación cuando surja una nueva vacante.
- Cumplir nuestras obligaciones en virtud de cualquier contrato laboral o relacionado con usted;
- Cumplir los requisitos legales aplicables y los códigos de buenas prácticas en materia de contratación y empleo (por ejemplo, la legislación sobre igualdad de oportunidades) y las obligaciones con terceros;
- Consultar la veracidad de su documento de identidad y demás datos proporcionados.
- Consultar las referencias laborales.
- Consultar mis datos en las listas restrictivas internacionales de lavado de activos y financiación de terrorismo y generar los reportes que al respecto sean requeridos por las autoridades competentes
- Gestionar las afiliaciones a la seguridad social como cotizante junto con sus beneficiarios.
- Administrar la relación laboral con usted y fines jurídicos, de personal, Administrativos y de gestión relacionados;
- Crear y mantener registros de personal y registros de enfermedad y ausencia para evaluar su capacidad laboral y tomar decisiones relativas a su aptitud para el trabajo;
- Recopilaremos y mantendremos datos sobre sus exámenes médicos y seguimiento de estado de salud, de acuerdo con los requerimientos legales, de salud ocupacional y recursos humanos.
- Administrar la nómina y pagar y revisar su salario y calcular, proporcionar y revisar sus prestaciones;
- Fines disciplinarios y/o de gestión del rendimiento;
- Ponerse en contacto con sus contactos de emergencia en caso de urgencia;
- Proporcionar referencias a bancos y otras instituciones financieras, arrendadores y/o futuros empleadores;
- Proporcionar información a organismos gubernamentales y cuasi-gubernamentales (incluyendo, sin limitación, fines fiscales, de seguridad social y otros similares);
- Combinar la información que recibimos de otras fuentes con la información que usted nos facilita y que nosotros recopilamos sobre usted y utilizar dicha información combinada para los fines antes indicados;

- Fines de gestión y seguridad del sitio, para que nuestros sitios web le resulten más útiles, para conocer el número de visitantes del sitio web y la tecnología que utilizan y para mejorar nuestro sitio web y asegurarnos de que el contenido se presenta de forma eficaz; y
- Administrar nuestros sitios web y para operaciones internas, incluida la resolución de problemas, el análisis de datos, las pruebas, la investigación y los fines estadísticos y de encuestas.
- Efectuar el control de cumplimiento de horario laboral, para lo cual se requieren los datos biométricos de los empleados.
- Efectuar el control ingreso y salida de las instalaciones de la empresa y protocolos de seguridad a través de datos biométricos (validar identidad, utilizar datos como factor de autenticación, recordar automáticamente los datos para el ingreso y logueo de acceso y salida, desarrollar e implementar procesos de seguridad y herramientas de prevención).
- Usar la foto para el carné de la compañía, huellas digitales, entre otras actividades de la organización.
- Monitoreo y grabación de las actividades que se desarrollen dentro de la compañía por cuestiones de seguridad, control subordinante por un máximo de 60 días, salvo, que amerite extender el tiempo de grabación como fines disciplinarios, sancionatorios, de gestión del rendimiento o investigaciones penales.
- Recolectar información de la labor ejecutada a través de monitoreo y grabación de llamadas y pantallas de equipos de la compañía
- Cumplir las obligaciones o ejercer facultades contractuales y legales.
- Conservar información del cumplimiento de obligaciones laborales y de la seguridad social, este ultimo de manera indefinida.
- Efectuar análisis estadísticos y demográficos.
- Consultar los datos personales relacionados con temas de salud, con el propósito de recibir información y acceder a los distintos servicios de los centros médicos, como: odontología, medicina general, especialidades médicas y campañas de promoción y prevención en salud ocupacional. Asimismo, para gestionar la transcripción de incapacidades o generación de reporte ante las ARL, COPASS o todas aquellas que las sustituyan en cumplimiento de la normatividad relacionada con seguridad social y seguridad y salud en el trabajo.
- Cualquier otra finalidad que corresponda según el vínculo que se genere entre los titulares de los datos personales y la compañía.

En vigencia del vínculo laboral o contractual, y después de su terminación, CALDIC podrá acceder y realizar tratamiento de los datos personales contenidos en correos electrónicos, carpetas y demás sistemas de almacenamiento registrados con los usuarios corporativos de los empleados para las finalidades establecidas en la política de protección de datos, así como la finalidad general de permitir el adecuado desarrollo de su actividad empresarial y garantizar el cumplimiento de sus obligaciones legales, principalmente en los ámbitos contable, tributario, legal, comercial y/o laboral.

En los casos que nos entregue datos personales de terceros titulares como familiares, el titular manifiesta que esta autorizado para proporcionar dichos datos y que los mismos serán tratados conforme a la política de protección de datos y acorde a las finalidades necesarias y razonables como contactos de emergencia, afiliaciones, beneficios de la empresa Cualquier otra finalidad que corresponda según el vínculo que se genere entre los titulares de los datos personales y la compañía.

Cómo compartimos sus datos personales

Además de las partes mencionadas anteriormente, también compartimos la información personal de nuestros solicitantes de empleo, empleados y/o colaboradores, según sea necesario, con los siguientes terceros:

- Cualquier miembro de nuestro grupo empresarial, es decir, nuestras filiales, nuestros holdings y sus filiales;
- Terceros seleccionados, como socios comerciales, asociados, asesores, proveedores, prestadores de servicios y subcontratistas (por ejemplo, proveedores de servicios informáticos y contables) para ejecutar los contratos que celebremos con ellos o con usted;
- Su familia, asociados y representantes, en su caso;
- Sus empleadores actuales, pasados y futuros, educadores y organismos examinadores;
- Agencias gubernamentales centrales y locales y otros organismos reguladores pertinentes
- Bancos y organizaciones financieras;
- Posibles compradores de nuestro negocio o activos, que pueden incluir su información personal;
- Cualquier otro tercero si es necesario para cumplir obligaciones legales, mandatos judiciales o hacer cumplir Acuerdos;
- Cualquier otro tercero si es necesario para proteger nuestros derechos, su propiedad o seguridad o los de otros.

Dónde transferimos y almacenamos la información personal

La información personal que recopilamos de nuestros solicitantes de empleo y empleados puede transmitirse, transferirse y almacenarse en territorio colombiano como en el exterior en servidores propios o de terceros contratados para su almacenamiento, garantizando una protección adecuada de dicha información personal y sensible.

La información personal y sensible que recabamos de usted también será tratada por personal que trabaja para nosotros o para alguno de nuestros proveedores. Esto incluye al personal que participa, entre otras cosas, en la prestación de servicios de apoyo.

Tomaremos todas las medidas razonablemente necesarias para garantizar que toda su información personal y sensible sea tratada de forma segura y de acuerdo con esta Política y la legislación aplicable, incluyendo la puesta en marcha de ciertas salvaguardas, incluyendo:

- Sólo el personal autorizado puede acceder a los datos personales y trabajar con ellos;
- Los datos personales deben almacenarse en carpetas especiales protegidas y controladas;
- El personal que trabaja con datos personales recibe formación sobre seguridad de la información
- Toda la información que nos proporcione se almacena en nuestros servidores seguros.

Cuando le hayamos proporcionado o usted haya elegido una contraseña que le permita acceder a determinadas partes de nuestros sitios web, *como empleado será responsable de mantener la confidencialidad de dicha contraseña*.

Por desgracia, la transmisión de información por Internet no es completamente segura. Aunque haremos todo lo posible por proteger su información personal, no podemos garantizar al 100% la seguridad de los datos transmitidos a nuestros sitios web; cualquier transmisión corre por su cuenta y riesgo.

Una vez recibida la información personal, utilizaremos procedimientos estrictos y elementos de seguridad para tratar de impedir el acceso no autorizado.

Ocasionalmente, nuestros sitios web pueden contener enlaces hacia y desde sitios web de terceros. Si sigue

un enlace a cualquiera de estos sitios web, tenga en cuenta que tienen sus propias políticas de privacidad y que no somos responsables de ellas. Consulte estas políticas antes de enviar datos personales a estos sitios web.

Retención

Almacenaremos su información personal durante periodos de tiempo limitados y adecuados, de acuerdo con nuestros calendarios de conservación aplicables*. Para mayor información remítase al título 6.8, 6.9 y 11 de esta política*.

Sus derechos

Usted tiene ciertos derechos respecto a la información personal que tenemos sobre usted. Los detalles de estos derechos figuran en la presente Política de Protección de Datos.

Para ejercer cualquiera de estos derechos, póngase en contacto con nosotros a través de los canales de atención descritos en la presente política.

Trataremos sus datos personales en consonancia con sus derechos, de acuerdo con la ley colombiana y únicamente de conformidad con ella (incluidos los plazos y requisitos aplicables en materia de tasas y cargos).

Propiedad del Documento

El Departamento Jurídico y de Cumplimiento asume la titularidad y responsabilidad de este documento, por tanto, garantiza que vela por su revisión oportuna y adecuada.

Anexo II:
Protección de Datos de Clientes y Proveedores

Este Anexo (y cualquier otro documento al que se haga referencia en él) establece las bases sobre las que **CALDIC** procesará y utilizará cualquier dato personal sobre nuestros Clientes y proveedores y clientes y proveedores potenciales que obtengamos de ellos, que ellos nos proporcionen o que obtengamos de terceros.

Para más información al respecto, consulte también nuestro Aviso de privacidad publicada en nuestro sitio web https://www.caldic.com/es-co

Información personal que recopila CALDIC y tratamiento lícito

CALDIC puede recopilar y utilizar varios tipos de datos personales sobre nuestros Clientes y proveedores y clientes y proveedores potenciales, incluidos los siguientes:

- Recopilaremos su título, nombre, segundo nombre, apellidos, información de contacto, incluida su dirección postal y código postal, dirección de correo electrónico y número de teléfono;
- Recopilaremos determinados datos financieros (por ejemplo, datos bancarios, información sobre cuentas financieras e información sobre tarjetas de pago);
- Podemos recopilar y utilizar otros datos personales cuando mantenemos correspondencia con usted (ya sea por teléfono, correo electrónico u otros medios).
- Podemos recopilar cierta información personal cuando nos comunique problemas con nuestro(s) sitio(s) web;
- Cuando visite nuestro(s) sitio(s) web, recopilaremos determinada información técnica sobre usted y su visita (por ejemplo, el dominio de Internet desde el que accede a nuestro(s) sitio(s) web, su dirección de protocolo de Internet, su tipo y versión de navegador, su sistema operativo y plataforma, las fechas y horas en que accede a nuestro(s) sitio(s) web, los sitios web o enlaces que utiliza para acceder a nuestro(s) sitio(s) web, la información de inicio de sesión, los detalles de los productos o servicios que consulta o busca y los localizadores uniformes de recursos ("URL") completos).
- Podemos recopilar datos sobre sus preferencias de marketing (por ejemplo, productos e intereses de mercado a través de nuestro sitio web) y si desea o no recibir determinados mensajes de marketing de nuestra parte (por ejemplo, correos electrónicos de marketing y boletines informativos) y si se obtiene/retira dicho consentimiento y en qué momento;
- Podemos recopilar cierta información que recibimos de otras fuentes con las que trabajamos estrechamente (por ejemplo, subcontratistas de servicios técnicos, de pago y de entrega, proveedores de motores de búsqueda, proveedores de análisis y socios comerciales);
- Recopilamos parte de su información personal directamente de usted;
- Necesitamos sus datos personales en relación con diversos requisitos contractuales relativos a determinadas normas sobre sanciones económicas.

Si no está dispuesto a facilitar dichos datos, es probable que no podamos cumplir las normas pertinentes aplicables en materia de sanciones económicas y/o cualesquiera otros controles o normas.

Recopilamos y utilizamos los datos personales de nuestros Clientes y Proveedores, así como de nuestros Clientes y Proveedores potenciales, ya que es necesario para nuestros intereses legítimos, así como para promocionar y vender nuestros bienes y servicios.

CALDIC

Finalidades del tratamiento de los datos personales de nuestros clientes y proveedores

Recopilamos y utilizamos datos personales de nuestros, Clientes y Proveedores actuales o anteriores y potenciales para los siguientes fines:

- Mantener comunicación constante y efectiva con los clientes, afiliados, proveedores, y cualquier persona respecto de la cual estemos autorizados para efectuar el tratamiento de sus datos personales.
- Proporcionarle los productos, servicios e información que nos solicite y cumplir nuestras obligaciones en virtud de los contratos que celebremos con usted;
- Mantener correspondencia y registrar cualquier comunicación;
- Enviarle boletines informativos por correo electrónico (puede darse de baja en cualquier momento utilizando los enlaces incluidos en los correos electrónicos o enviando un correo electrónico a privacy_col@caldic.com y facilitarle información comercial sobre nuestros servicios, en cada caso si está de acuerdo;
- Fines de gestión y seguridad del sitio, para que nuestros sitios web le resulten más útiles, para conocer el número de visitantes del sitio web y la tecnología que utilizan y para mejorar nuestro sitio web y asegurarnos de que el contenido se presenta de forma eficaz; y
- Administrar nuestros sitios web y para operaciones internas, incluida la resolución de problemas, el análisis de datos, las pruebas, la investigación y los fines estadísticos y de encuestas.
- Informarle sobre cambios en nuestros productos y/o servicios;
- Cumplir la legislación, los reglamentos y los códigos de buenas prácticas aplicables, y con fines jurídicos, administrativos y de gestión;
- Facilitar información a organismos gubernamentales y reguladores con fines fiscales y otros similares.
- Invitar a eventos organizados por CALDIC, compañías vinculadas y terceros, organizar concursos y otorgar premios.
- Desarrollar actividades comerciales conjuntas con compañías o entidades vinculadas o aliadas.
- Mantener información sobre Peticiones, quejas y reclamos presentados por los clientes y proveedores afiliados con ocasión de actividades desarrolladas por la compañía.
- Conservar información relacionada con el cumplimiento de obligaciones contractuales y en todos los ámbitos legales de la empresa CALDIC.
- Efectuar análisis estadísticos, demográficos y de mercado.
- Elaboración de estudios y publicaciones de carácter académico y periodístico relacionadas con las actividades de la empresa CALDIC, y el mercado que atiende.
- Acreditar experiencia en contratación pública y/o privada.
- Cumplir con las obligaciones que la empresa CALDIC, tenga a cargo o sobre la cual pueda exigir cumplimiento.
- Obtener un registro o licencia de importación ante Invima, Ica y ministerio de justicia.
- Expedir certificaciones y recomendaciones comerciales.
- Monitoreo y grabación de las actividades que se desarrollen dentro de la compañía por cuestiones de seguridad, por un máximo de 60 días, salvo causa justificada, que amerite extender el tiempo de grabación.
- Recolectar información de datos biométricos para control de acceso y salida de cualquier instalación de la compañía
- Recolectar información de vínculos a entidades de seguridad social, para la atención de

emergencias y/o verificación del cumplimiento de obligaciones legales.

- Cualquier otra finalidad que corresponda según el vínculo que se genere entre los titulares de los datos personales y la compañía, tales como procesos de cobro y seguimiento de cartera.
- Reportar información tributaria o legal conforme a la legislación vigentes.
- Consultar mis datos en las listas restrictivas internacionales de lavado de activos y financiación de terrorismo y generar los reportes que al respecto sean requeridos por las autoridades competentes.
- Compartir los datos relativos a la información financiera, lo cual incluye el uso y la actualización de los datos de contacto, con firmas especializadas en labores de cobranzas para que adelanten la gestión de cobro y recaudo de las obligaciones contraídas, y demás servicios que se consideren necesarios o complementarios. Así como, el manejo de la cartera vencida, utilizando para ello tanto los mecanismos judiciales como también las vías extraprocesales permitidas por el ordenamiento jurídico.
- Consultar, solicitar y/o verificar el comportamiento comercial, crediticio, financiero, y de servicios en los Operadores de Información (entendidos estos como los Operadores de qué trata la Ley 1266 de 2008 y demás normas que la complementen, modifiquen, adicionen o sustituyan).

Cómo compartimos sus informaciones personales

Además de las partes mencionadas anteriormente, también compartimos la información personal de nuestros Clientes y Proveedores y de nuestros Clientes y Proveedores potenciales, según sea necesario, con las siguientes terceras partes:

- Cualquier miembro de nuestro grupo, es decir, nuestras filiales, nuestra holdings y sus filiales;
- Terceros seleccionados, incluidos socios comerciales y proveedores de servicios (por ejemplo, proveedores de servicios informáticos, contables, técnicos, de pago y de entrega) para ejecutar cualquier contrato que celebremos con ellos o con usted para suministrar nuestros bienes y servicios;
- Posibles compradores de nuestro negocio o activos, que pueden incluir su información personal;
- Cualquier otro tercero si es necesario para cumplir obligaciones legales o hacer cumplir Acuerdos;
- Cualquier otro tercero si es necesario para proteger nuestros derechos, su propiedad y/o seguridad o los de otros.

Dónde transferimos y almacenamos la información personal

Trabajamos para garantizar que los datos personales pueden almacenarse y/o transferirse tanto en el territorio colombiano como en el exterior en servidores propios o de terceros contratados para su almacenamiento, garantizando una protección adecuada de dicha información personal y sensible.

La información personal y sensible que recabamos de usted también será tratada por personal que trabaja para nosotros o para alguno de nuestros proveedores. Esto incluye al personal que participa, entre otras cosas, en la prestación de servicios de apoyo.

Adoptaremos todas las medidas razonablemente necesarias para garantizar que toda su información personal se trate de forma segura y de conformidad con la legislación aplicable, entre otras cosas, mediante la implantación de determinadas garantías, entre las que se incluyen:

- Sólo el personal autorizado puede acceder a los datos personales y trabajar con ellos;
- Los datos personales deben almacenarse en carpetas especiales protegidas y controladas;

- El personal que trabaja con datos personales ha recibido formación en seguridad de la información. Toda la información que nos facilita se almacena en nuestros servidores seguros.

Todas las transacciones de pago estarán encriptadas. Cuando le hayamos proporcionado o usted haya elegido una contraseña que le permita acceder a determinadas partes de nuestros sitios web, será responsable de mantener la confidencialidad de dicha contraseña.

Por desgracia, la transmisión de información por Internet no es completamente segura. Aunque haremos todo lo posible por proteger su información personal, no podemos garantizar la seguridad de los datos transmitidos a nuestros sitios web; cualquier transmisión corre por su cuenta y riesgo.

Una vez recibida la información personal, utilizaremos procedimientos estrictos y elementos de seguridad para tratar de impedir el acceso no autorizado.

Ocasionalmente, nuestros sitios web pueden contener enlaces hacia y desde sitios web de terceros. Si sigue un enlace a cualquiera de estos sitios web, tenga en cuenta que tienen sus propias políticas de privacidad y que no somos responsables de ellas. Consulte estas políticas antes de enviar datos personales a estos sitios web.

Retención

Almacenaremos su información personal durante periodos de tiempo limitados y adecuados, de acuerdo con nuestros calendarios de conservación aplicables*. Para mayor información remítase al título 6.8, 6.9 y 8 de esta política*.

Sus derechos

Usted tiene ciertos derechos con respecto a la información personal que tenemos sobre usted. Los detalles de estos derechos figuran en esta Política.

Para ejercer cualquiera de estos derechos, póngase en contacto con nosotros a través de los canales de atención descritos en la presente política.

Trataremos toda la información personal en consonancia con sus derechos, en cada caso en la medida en que lo exija la legislación aplicable y únicamente de conformidad con ella (incluido el cumplimiento de los plazos aplicables y de cualquier requisito relativo a tasas y cargos).

Anexo III:
Retención

Cualquiera que trate datos personales debe cumplir ciertos principios de buenas prácticas, entre ellos que los datos personales no deben conservarse más tiempo del necesario para los fines para los que fueron recogidos, salvo determinadas excepciones.

Esto abarca los datos personales incluidos en cualquier registro que conservemos. Un registro de datos personales es cualquier tipo de información personal creada, recibida o transmitida en la transacción de nuestro negocio, independientemente del formato físico (los registros pueden estar en papel o en formato electrónico).

Para cumplir este principio, debemos:

- No conservar los datos personales más tiempo del necesario para los fines para los que fueron recogidos;
- Establecer y cumplir periodos adecuados de conservación de datos personales (que pueden determinarse para satisfacer requisitos legales, contables u otros requisitos normativos), salvo determinadas excepciones;
- Tomar todas las medidas razonables para destruir de forma segura, o borrar de nuestros sistemas, todos los datos personales que ya no sean necesarios;
- Revisar periódicamente los datos personales que conservamos para garantizar que los periodos de conservación son adecuados.

Excepciones

Exigimos a todo el personal que cumpla íntegramente los calendarios y procedimientos de conservación previstos en esta política.

No obstante, todo el personal debe tener en cuenta la siguiente excepción general a cualquier calendario de destrucción establecido:

- Si el usuario de datos cree, o el departamento Jurídico y de Cumplimiento le informa, que nuestros registros de datos personales son relevantes para un litigio en curso, un litigio potencial, una investigación gubernamental, una auditoría u otro acontecimiento, debe conservar y no borrar, eliminar, destruir o modificar dichos registros, incluidos los correos electrónicos, hasta que el departamento de Cumplimiento determine que dichos registros ya no son necesarios;
- Esta excepción sustituye a cualquier calendario de destrucción de dichos registros establecido con anterioridad o posteriormente; y
- Cuando se crea que puede aplicarse esta excepción, o si tiene alguna pregunta, póngase en contacto con el departamento Jurídico y de Cumplimiento

También se le puede pedir que suspenda cualquier procedimiento rutinario de eliminación de documentos de datos personales en relación con otros tipos de acontecimientos, como la fusión de **CALDIC** con otra organización o la sustitución de nuestros sistemas de tecnología de la información.

Propiedad del Documento

El Departamento Jurídico y de Cumplimiento asume la titularidad y responsabilidad de este documento, por tanto, garantiza que vela por su revisión oportuna y adecuada.

Anexo IV:
Seguridad de los Datos

La seguridad de los datos es la práctica de garantizar la seguridad, confidencialidad, integridad y disponibilidad de los datos personales que recopilamos, creamos, mantenemos, almacenamos, transmitimos y/o utilizamos.

Su objetivo es proteger frente a cualquier amenaza o peligro previstos para la seguridad, confidencialidad, integridad o disponibilidad de dichos datos personales y proteger frente al acceso o uso no autorizados de los datos personales que procesamos, que podrían provocar daños sustanciales o riesgo de usurpación de identidad o fraude.

En **CALDIC** existe un programa definido de seguridad de datos personales que gestiona nuestro departamento de TI. Hemos designado a un responsable de seguridad que forma parte del departamento de TI.

El Responsable de Seguridad es responsable de aplicar, coordinar y mantener las medidas de seguridad de los datos, que incluyen:

- Aplicación inicial de esta Política, lo que implicará, por ejemplo:

    - Evaluar los riesgos internos y externos para nuestros sistemas y datos personales y mantener la documentación correspondiente, incluidos los informes de evaluación de riesgos y los planes de corrección;
    - Coordinar el desarrollo, distribución y mantenimiento de las políticas y procedimientos de seguridad de la información;
    - Coordinar el diseño de garantías administrativas, técnicas y físicas razonables y adecuadas para proteger los datos personales;

El responsable de seguridad también se asegura de que se apliquen y mantengan las garantías para proteger los datos personales en toda nuestra organización, cuando proceda:

- Supervisar a los empleados, miembros del consejo de administración, proveedores de servicios y contratistas independientes que acceden a los datos personales o los conservan en nuestro nombre;
- Seguimiento y comprobación continuos de la aplicación y la eficacia;
- Definir y gestionar los procedimientos de respuesta a incidentes;
- Proporcionar formación periódica sobre nuestras garantías y las políticas y procedimientos de seguridad de la información pertinentes a todo el personal y (en su caso) a las partes interesadas que tengan o puedan tener acceso a datos personales;
- Garantizar que los asistentes a la formación acusen recibo y comprendan formalmente la formación y la documentación relacionada, mediante formularios de acuse de recibo por escrito;
- Conservar los registros de formación y reconocimiento; y
- Evaluar la capacidad de nuestros terceros proveedores de servicios (incluidos los encargados del tratamiento de datos) para aplicar y mantener medidas de seguridad adecuadas para los datos personales a los que les permitimos acceder y

exigirles contractualmente que apliquen y mantengan dichas medidas;

- Definir y gestionar un proceso de excepciones para revisar, aprobar o denegar, documentar, supervisar y reevaluar periódicamente cualquier solicitud de desviación de esta Política que resulte necesaria y adecuada en función de la actividad empresarial, y

a) Informar periódicamente a nuestra dirección sobre el estado de nuestro programa de seguridad de la información y nuestras garantías para proteger los datos personales.

CALDIC adoptará todas las medidas necesarias para garantizar un alto estándar de seguridad en el manejo de los datos e información que trate como responsable o encargado. No obstante, considerando la naturaleza de la actividad y los constantes cambios en los sistemas de almacenamiento y los avances tecnológicos asociados, no es posible asegurar un nivel de seguridad completamente infalible.

De igual manera, **CALDIC** firmará acuerdos con empleados, contratistas y en general colaboradores para asegurar el cumplimiento adecuado de la presente política y nuestras directrices en materia de seguridad de la información. No obstante, **CALDIC** no asumirá responsabilidad alguna por el uso indebido de los datos que se realice en contravención a los acuerdos u obligaciones pactadas con estos.

Evaluación de riesgos

CALDIC realiza evaluaciones de riesgos periódicas y documentadas. La evaluación de riesgos deberá:

- Identificar los riesgos internos y externos razonablemente previsibles para la seguridad, confidencialidad, integridad o disponibilidad de cualquier registro electrónico, en papel o de otro tipo de datos personales;
- Evaluar la probabilidad y los daños potenciales que podrían derivarse de tales riesgos, teniendo en cuenta la sensibilidad de los datos personales;
- Evaluar la adecuación de las políticas, procedimientos, sistemas y garantías pertinentes establecidos para controlar dichos riesgos, en ámbitos que incluyen, por ejemplo:

a) Formación y gestión del personal y las partes interesadas
b) Cumplimiento de esta política y de las políticas y procedimientos conexos por parte del personal y las partes interesadas
c) sistemas de información, incluida la adquisición, el diseño, la aplicación, las operaciones y el mantenimiento de redes, ordenadores y programas informáticos, así como el tratamiento, almacenamiento, transmisión, conservación y eliminación de datos, y
d) nuestra capacidad para prevenir, detectar y responder a ataques, intrusiones y otros incidentes de seguridad o fallos del sistema.

Tras cada evaluación de riesgos, **CALDIC** va a:

- Diseñar, aplicar y mantener garantías razonables y adecuadas para minimizar los riesgos identificados;
- Abordar de forma razonable y adecuada las lagunas detectadas; y
- Supervisar periódicamente la eficacia de nuestras garantías, tal como se especifica en la presente Política

Políticas y procedimientos de seguridad de la información

Desarrollaremos, mantendremos, distribuiremos al personal pertinente y a otras partes interesadas y revisaremos las políticas y procedimientos de seguridad de la información de conformidad con las leyes y normas aplicables.

El proceso será dirigido por el responsable de seguridad, que informará exhaustivamente a nuestra dirección de los resultados y recomendaciones de seguridad derivados de las revisiones. El proceso incluye el establecimiento de políticas relativas a:

- Clasificación de información
- Las prácticas de tratamiento de datos personales, incluidos el almacenamiento, el acceso, la eliminación y la transferencia externa o el transporte de datos personales
- Gestión del acceso de los usuarios, incluida la identificación y autenticación (mediante contraseñas u otros medios adecuados)
- Encriptación
- Seguridad informática y de redes
- Seguridad física
- Notificación y respuesta a incidentes
- Uso de la tecnología por parte del personal, incluido el uso aceptable y el uso de dispositivos propios; y
- Adquisición, desarrollo, operaciones y mantenimiento de sistemas de información

El proceso también incluye detallar la aplicación y el mantenimiento de nuestras garantías administrativas, técnicas y físicas.

Garantías generales y administrativas

Desarrollaremos, aplicaremos y mantendremos garantías administrativas, técnicas y físicas razonables de conformidad con las leyes y normas aplicables para proteger la seguridad, confidencialidad, integridad y disponibilidad de los datos personales que poseemos.

Las garantías deberán ser adecuadas a nuestro tamaño, alcance y actividad, a nuestros recursos disponibles y a la cantidad de datos personales que conservamos o mantenemos en nombre de terceros, reconociendo al mismo tiempo la necesidad de proteger tanto la información de los Clientes como la del Personal.

Documentaremos nuestras garantías administrativas, técnicas y físicas en nuestras políticas y procedimientos de seguridad de la información.

Nuestras garantías administrativas incluirán, como mínimo:

- Designar a uno o varios miembros del personal para coordinar el programa de seguridad de la información;
- Limitar la cantidad de datos personales recogidos a la razonablemente necesaria para cumplir nuestros fines empresariales legítimos, o para cumplir la legislación aplicable;
- Limitar el acceso a los registros de datos personales a aquellas personas que

razonablemente deban conocer dicha información para cumplir nuestro legítimo propósito comercial o permitirnos cumplir la legislación aplicable;

- Identificar los riesgos internos y externos razonablemente previsibles, y evaluar si las garantías existentes controlan adecuadamente dichos riesgos;
- Formación del personal en prácticas y procedimientos del programa de seguridad, con supervisión de la dirección;
- Seleccionar proveedores de servicios (incluidos, entre otros, los encargados del tratamiento de datos) capaces de mantener las garantías adecuadas, y exigirles contractualmente que lo hagan, y;
- Ajustar nuestro programa de seguridad de la información a la luz de los cambios empresariales o de nuevas circunstancias.

Garantías técnicas

Nuestras garantías técnicas incluirán el mantenimiento de un sistema de seguridad que cubra nuestra red (incluidas las capacidades inalámbricas) y ordenadores que, como mínimo, y en la medida en que sea técnicamente factible, soporten:

- **Protocolos seguros de autenticación de usuarios, incluidos:**
    - Controlar la identificación y autenticación de los usuarios con métodos razonablemente seguros de asignación y selección de contraseñas (garantizando que las contraseñas se guardan en un lugar/formato que no comprometa la seguridad) o mediante el uso de otras tecnologías, como la biometría o los dispositivos token;
    - Restringir el acceso únicamente a los usuarios activos y a las cuentas de usuario activas, lo que incluye impedir que el personal cesado acceda a los sistemas o registros; y
    - Bloquear el acceso a determinados identificadores de usuario tras varios intentos infructuosos de acceder o imponer limitaciones de acceso al sistema en cuestión;

- **Medidas de control de acceso seguro, incluyendo:**
    - Restringir el acceso a los registros y ficheros que contengan datos personales a quienes necesiten conocerlos para desempeñar sus funciones; y
    - Asignar identificadores y contraseñas únicos (u otros medios de autenticación, pero no contraseñas predeterminadas suministradas por el proveedor) a cada persona con acceso a ordenadores o redes que estén razonablemente diseñados para mantener la seguridad;

Nuestras garantías técnicas incluirán el mantenimiento de un sistema de seguridad que cubra nuestra red (incluidas las capacidades inalámbricas) y ordenadores que, como mínimo, y en la medida en que sea técnicamente factible, admita:

- Cifrado de todos los datos personales que viajan de forma inalámbrica o a través de redes públicas, o que se almacenan en ordenadores portátiles u otros dispositivos portátiles o móviles;
- Supervisión razonable del sistema para prevenir, detectar y responder al uso o acceso no autorizado

a datos personales u otros ataques o fallos del sistema;
- Protección de cortafuegos y parches de software razonablemente actualizados para los sistemas que contengan (o puedan proporcionar acceso a sistemas que contengan) datos personales; y

- Software de seguridad del sistema razonablemente actual (o una versión que pueda seguir siendo compatible) que: (i) incluya protección contra software malicioso ("malware") con parches y definiciones de malware razonablemente actuales; y (ii) esté configurado para recibir actualizaciones de forma periódica.

Garantías físicas

Nuestras garantías físicas deberán, como mínimo, prever:

- Definir y aplicar medidas razonables de seguridad física para proteger las zonas en las que se pueda acceder a los datos personales, lo que incluye restringir razonablemente el acceso físico y almacenar los registros de datos personales en instalaciones, zonas o contenedores cerrados con llave;
- Prevenir, detectar y responder a intrusiones o accesos no autorizados a datos personales, incluso durante o después de su recogida, transporte o eliminación;
- Eliminar o destruir de forma segura los datos personales, ya sea en papel o en formato electrónico, cuando ya no deban conservarse de conformidad con la legislación aplicable o las normas aceptadas.

Respuesta a incidentes

Hemos establecido y mantenemos políticas y procedimientos relativos a la respuesta a incidentes de seguridad de la información. Dichos procedimientos incluyen:

- Establecer una estructura de notificación de incidentes en la que el personal deba notificar al Responsable de Seguridad y al departamento Jurídico y de Cumplimiento en caso de que se conozca o sospeche un incidente de seguridad relacionado datos personales;
- Determinar la respuesta requerida ante una posible violación de los datos personales, incluida la posible notificación a las personas y a la Superintendencia de Industria y Comercio;
- Documentar la respuesta a cualquier incidente o suceso que implique una violación de la seguridad;
- Realizar una revisión posterior al incidente de los acontecimientos y las medidas adoptadas; y
- Abordar de forma razonable y adecuada las lagunas detectadas.

Propiedad del Documento

El Departamento Jurídico y de Cumplimiento asume la titularidad y responsabilidad de este documento, por tanto, garantiza que vela por su revisión oportuna y adecuada.

Anexo V:
Incidentes de Seguridad

Un "incidente de seguridad" relacionado con datos personales, es cualquier violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la difusión o el acceso no autorizados, de datos personales transmitidos, conservados o tratados de otra forma por **CALDIC.**

Los incidentes de seguridad relacionados con el tratamiento de datos personales son cada vez más frecuentes y pueden producirse de diversas maneras, algunos ejemplos no exhaustivos de cómo pueden producirse Los incidentes de seguridad relacionados con el tratamiento de datos personales son:

- Pérdida o robo de documentos que contengan datos personales o de equipos en los que se almacenen datos personales (por ejemplo, documentos en papel, ordenadores portátiles, teléfonos inteligentes o unidades USB que contengan datos personales y que se hayan dejado accidentalmente en lugares públicos, o que hayan sido robados en nuestros locales);
- Acceso o uso no autorizado de nuestros datos (por ejemplo, si un miembro del personal accede a datos personales cuando no está autorizado para ello, o que no son necesarios para su función concreta, o si se hace un uso no autorizado de la contraseña o tarjeta de acceso de un miembro del personal, o si se envían datos personales a un tercero sin autorización);
- Fallo de los equipos (por ejemplo, si fallan nuestros servidores, lo que provoca la pérdida o corrupción de datos personales, o si fallan nuestros cortafuegos, lo que permite a terceros no autorizados acceder a nuestros sistemas);
- Error humano, (por ejemplo, si se enviaron datos personales a un destinatario no autorizado o incorrecto por correo electrónico, carta o fax, o se perdió una tarjeta llave de la oficina que permitió a un tercero no autorizado acceder a zonas seguras de nuestros locales en las que había datos personales accesibles o visibles);
- Destrucción insegura de documentos o soportes que contengan datos personales (por ejemplo, si para la eliminación de documentos se utilizan contenedores no seguros en lugar de contenedores seguros para la trituración/eliminación y destrucción de documentos confidenciales);
- Incumplimiento de nuestras políticas de protección de datos, privacidad, conservación de datos personales o seguridad de los datos personales;
- Acontecimientos que escapen a nuestro control (por ejemplo, si se produce un incendio o una inundación que provoque el fallo de los equipos o la destrucción de los datos personales);
- Ataques de piratas informáticos que den lugar a que terceros obtengan acceso no autorizado a nuestros sistemas informáticos y datos personales; y
- Delitos de "phishing" en los que la información se obtiene de nosotros mediante engaño, (por ejemplo, si un tercero se hace pasar por un miembro del Personal o un Cliente para obtener acceso no autorizado a datos personales o se envía un correo electrónico de "phishing" al Personal que conduce a una infección por malware de nuestros Sistemas de TI);
- Fallo de los equipos (por ejemplo, si fallan nuestros servidores, lo que provoca la pérdida o corrupción de datos personales, o si fallan nuestros cortafuegos, lo que permite a terceros no autorizados acceder a nuestros sistemas).
- El secuestro de datos mediante ataques de ransomware supone que un atacante introduce software malicioso que cifra la información crítica de la organización, impidiendo el acceso

legítimo hasta que se pague un rescate. Este tipo de incidente no solo paraliza operaciones y pone en riesgo la disponibilidad de los datos personales, sino que puede derivar en su divulgación pública si no se accede a las exigencias del atacante, lo que vulnera gravemente la confidencialidad y la integridad de la información tratada.

- Vulnerabilidades de configuración, se producen cuando sistemas, aplicaciones o servicios en la nube quedan expuestos por ajustes erróneos (por ejemplo, permisos abiertos en repositorios o buckets sin protecciones adecuadas), lo que permite a usuarios no autorizados acceder, modificar o extraer datos personales. Estos errores de configuración pueden deberse a políticas de acceso demasiado laxas, credenciales predeterminadas sin cambiar o falta de cifrado en tránsito y reposo, y comprometen la confidencialidad y la integridad de la información al facilitar el acceso no controlado a los datos.
- Brechas de proveedores o terceros aquellos incidentes de seguridad originados en socios, proveedores o servicios subcontratados que, teniendo acceso a datos personales por cuenta de GTM, sufran vulneraciones o fallos en sus controles y deriven en la divulgación, alteración o pérdida de la información. Para mitigarlas, se incluirán cláusulas de seguridad y notificación en los contratos, se evaluará periódicamente el nivel de protección de los terceros y se exigirá la aplicación de estándares equivalentes a los de GTM en materia de confidencialidad, integridad y disponibilidad.
- Errores en actualizaciones o parches de seguridad aquellos fallos derivados de la aplicación incorrecta, incompleta o tardía de actualizaciones críticas en sistemas, aplicaciones o dispositivos, que dejen vulnerabilidades sin corregir y permitan a atacantes comprometer la confidencialidad, integridad o disponibilidad de los datos personales. Para evitarlos, mantendremos un programa de gestión de parches que incluya fases de prueba previas, aprobación formal, despliegue coordinado y registro de cada actualización, así como revisiones periódicas para garantizar que todos los componentes cuenten con las versiones más seguras.

Riesgos de los Incidentes de seguridad de datos personales

Los incidentes de seguridad relacionados con datos personales pueden tener una serie de consecuencias adversas, tanto para los sujetos de los datos afectados por la violación como para **CALDIC**

Los incidentes de seguridad relacionados con datos personales pueden provocar angustia emocional y/o diversos tipos de daños físicos y/o financieros a las personas, entre ellos:

- Pérdida de control sobre sus datos personales (por ejemplo, que se conozca información sobre la vida privada de una persona, como la limitación de su derecho a la intimidad;
- Discriminación;
- Robo de identidad, fraude y/o pérdidas financieras;
- Daños a la reputación;
- Otras desventajas económicas o sociales para el sujeto de los datos.

Los incidentes de seguridad relacionados con datos personales también pueden acarrear una serie de consecuencias adversas para **CALDIC**, entre las que se incluyen:

- Pérdida de la confianza de nuestros empleados, Clientes y/o proveedores;
- Medidas coercitivas, incluidas importantes sanciones económicas;
- Particulares que emprendan acciones contra CALDIC y reclamen indemnizaciones (incluso a través de procedimientos de tipo acción de grupo); y

- Importantes daños a la reputación y publicidad negativa.

Notificaciones

Cuando se produzca un incidente de seguridad relacionado con datos personales, estamos obligados a notificarlo a la Superintendencia de Industria y Comercio como autoridad de protección de datos en Colombia, dentro del plazo establecidos por en el Título Quinto de la Circular Única de la Superintendencia de Industria y Comercio, es decir, 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, estemos o no obligados a registrar bases de datos en el RNBD.

Una notificación a una autoridad de control debe incluir cierta mínima información.

También debemos documentar cualquier incidente de seguridad relacionado con el tratamiento de los datos personales que se produzca.

En función de la naturaleza de la infracción, es posible que también tengamos que informar de ella a otros terceros (por ejemplo, entidades financieras, aseguradoras, sindicatos, organismos profesionales, otros reguladores y/o autoridades policiales).

Qué hacer si tiene conocimiento de un incidente de seguridad relacionado con el tratamiento de los datos personales

Si descubre, tiene conocimiento o sospecha de que se está produciendo o se ha producido un incidente de seguridad relacionado con el tratamiento de los datos personales , debe hacerlo:

- ***Siempre*** *póngase en contacto* ***de inmediato*** con el departamento de TI y con el departamento Jurídico y de Cumplimiento (Correo: privacy_col@caldic.com), incluso si no está seguro de que se haya producido una violación o de si la violación afecta o no a datos personales; y
- Cooperar plenamente con cualquier investigación o respuesta a cualquier infracción confirmada o sospechada y cumplir con cualquier instrucción del departamento de TI y Jurídico y de Cumplimiento tan pronto como sea posible para garantizar que cumplimos con nuestras obligaciones en virtud de la normatividad: artículo 15 de la Constitución Política (derecho a la intimidad y al buen nombre), la Ley 1266 de 2008 (habeas data financiero), la Ley 1581 de 2012 (protección de datos personales) y su reglamentación a través del Decreto Único Reglamentario 1074 de 2015, así como la Ley 1273 de 2009 (delitos informáticos), la Ley 527 de 1999 (comercio electrónico y firma digital), la Circular 02 de 2015 de la SIC (seguridad de la información) y las directrices específicas que para IA expida la autoridad competente y las demás normatividad aplicable en Colombia y el GRPD en los casos en que sea aplicable.

Los departamentos de TI, Jurídico y de Cumplimiento son responsables de:

- Reportar los incidentes de seguridad relacionados con el tratamiento de datos personales a la Superintendencia de Industria y Comercio, a las personas afectadas por la violación y/o a terceros;
- Decidir si se está produciendo o se ha producido una infracción en casos poco claros;

- Gestionar cualquier violación o sospecha de violación de los datos personales y ponerse en contacto con el personal pertinente y otros terceros para obtener información de ellos;
- Investigar, contener y recuperar, evaluar los riesgos de, evaluar, responder a y documentar la violación pertinente, y
- Notificar la infracción a la autoridad de control competente, a las personas afectadas por la infracción y a las autoridades competentes y de ser necesario a otros terceros titulares de los datos.

A menos que esté específicamente autorizado para ello por el departamento de TI o el departamento Legal y de Cumplimiento, ***no debe hacerlo bajo ninguna circunstancia***:

- Emprender cualquiera de las acciones de las que es responsable el departamento de TI o Jurídico y de Cumplimiento, según lo expuesto anteriormente; o
- Revelar de otro modo detalles de (incluida la existencia o sospecha de existencia de) cualquier incidente de seguridad relacionado con el tratamiento de los datos personales a cualquier otra persona o tercero (incluido nuestro otro personal) que no sea el departamento de TI o Jurídico y de Cumplimiento.

Para más información y orientación sobre incidentes de seguridad relacionados con el tratamiento de datos personales y/o nuestras medidas de seguridad de datos personales, póngase en contacto con el area encargada de protección de datos personales o el departamento de TI o con el departamento Jurídico y de Cumplimiento (Correo: Privacy_col@caldic.com).

Propiedad del Documento

El Departamento Jurídico y de Cumplimiento asume la titularidad y responsabilidad de este documento, por tanto, garantiza que vela por su revisión oportuna y adecuada.