Política Tratamiento de Datos Personales

Visum TIC Group SAS

2024

1. BASE LEGAL Y ÁMBITO DE APLICACIÓN

1.1. Ámbito de aplicación:

La presente política aplica sobre los datos personales tratados en la sociedad **Visum TIC Group SAS**, sociedad legalmente constituida identificada con el Nit 901872098-0, en cumplimiento con la Ley 1581 de 2012 y demás normatividad vigente en materia de protección de datos personales. Esta política es de obligatorio conocimiento y cumplimiento para nuestros colaboradores, contratistas y proveedores, así como a cualquier otra parte que realice tratamiento de datos personales bajo nuestra responsabilidad. Se exceptúan de este alcance los casos establecidos por el artículo 2 de la Ley 1581 de 2012 y las normas que lo modifiquen, deroguen o subroguen.

1.2. Objeto:

La presente política tiene como objeto brindar la información necesaria a los Titulares de los datos y terceros interesados, acerca de las condiciones del tratamiento de los datos personales que son suministrados a la sociedad, así como, establecer las directrices que serán aplicadas en las actividades de recolección, almacenamiento, uso, circulación, y supresión de datos personales para garantizar su protección y los derechos de sus Titulares.

1.3. Normatividad Aplicable:

La presente política ha sido elaborada con fundamento en la normatividad vigente en materia de protección de datos personales, esencialmente la siguiente:

- Constitución Política de Colombia
- Ley Estatutaria 1581 de 2012
- Decreto 1074 de 2015 Capitulo 25 y Capitulo 26 compilatorio de los decretos:
  - Decreto 1377 de 2013
  - Decreto 886 de 2014
- Ley 1266 de 2008 “Por la cual se dictan las disposiciones generales del Habeas Data”.
- Actos administrativos expedidos por la Superintendencia de Industria y Comercio.

2. RESPONSABLE DEL TRATAMIENTO

La sociedad **Visum TIC Group SAS**, identificada con el Nit 901872098-0, actúa en la presente política como Responsable del Tratamiento. Los datos de contacto son los siguientes:

Dirección: Calle 26A No. 13 97. Oficina 1501. Edificio Bulevar Tequendama. Centro Internacional.
Teléfono de contacto: 3133688289
Correo electrónico: info@visumtic.com consultoria@visumtic.com

3. DEFINICIONES

1. Anonimización: Es el proceso mediante el cual se eliminan o modifican los datos personales de tal manera que el dato personal no pueda ser asociado con una persona natural identificable, utilizando cualquier medio, tecnología o proceso que permita se desvincular o desasociar los datos.

2. Autorización: Manifestación de voluntad previa, voluntaria y expresa del Titular de los datos personales, mediante la cual acepta el tratamiento de sus datos para una o varias finalidades específicas.

3. **Aviso de privacidad:** Comunicación verbal o escrita generada por el Responsable o Encargado, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las Políticas de Tratamiento de datos personales que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

4. Base de Datos: Conjunto organizado de datos personales que son objeto de tratamiento por parte de la entidad, de acuerdo con las finalidades establecidas por la organización.

5. Dato Personal: Cualquier información vinculada o que pueda asociarse a una persona natural identificada o identificable.

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

7. Dato personal público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público.

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

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

10. Oficial de protección de datos: Es la persona natural o jurídica designada para la implementación efectiva de las políticas y procedimientos en aplicación del Régimen de Protección de Datos Personales de Colombia. Así mismo, promueve la implementación de buenas prácticas en la gestión y administración de datos personales en las distintas áreas y procesos en la sociedad.

11. 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.

12. Titular de los datos: Persona natural cuyos datos personales sean objeto de tratamiento.

13. Transferencia de datos: La transferencia de datos tiene lugar cuando el Responsable Tratamiento de datos personales desde un país emisor de los datos, envía los datos personales a un receptor que se encuentra ubicado en un territorio distinto, que a su vez es Responsable del Tratamiento.

14. Transmisión: Tratamiento de datos personales que implica la comunicación de estos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento determinado por el encargado por cuenta del responsable.

4. PRINCIPIOS DE LA PROTECCIÓN DE DATOS

A continuación, se identifican los principios que rigen de manera armónica e integral la protección de datos personales según el artículo 4º de la Ley 1581 de 2012:

1. Principio de legalidad: El tratamiento de los datos personales se realizará cumpliendo con la normativa legal vigente, respetando los derechos del Titular, se trata de una actividad reglada que debe sujetarse a lo establecido en las disposiciones legales que la desarrollen.

2. Principio de finalidad: El Tratamiento de los datos debe obedecer a una finalidad legítima, expresamente aprobada por el Titular, garantizando que sean compatibles con la constitución y la Ley.

3. Principio de libertad: El Tratamiento sólo 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.

4. Principio de veracidad o calidad: Los datos personales sujetos a tratamiento deben conservarse garantizando un procesamiento veraz, completo, exacto, actualizado, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

5. Principio de transparencia: El Titular debe ser informado de manera clara y completa sobre el tratamiento de sus datos personales y garantizarse su derecho 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.

6. Principio de acceso y circulación restringida: El acceso a los datos personales estará restringido a las personas autorizadas para su tratamiento, garantizando la confidencialidad y privacidad. El Tratamiento de los datos sólo podrá ser realizado por personas autorizadas por el titular o en la ley. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados.

7. Principio de Seguridad: La información sujeta a Tratamiento por el responsable o el Encargado de este y al a que se refiere la Ley 1581 de 2012, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Se implementarán medidas técnicas y organizativas para proteger los datos personales frente a pérdida, acceso no autorizado,

alteración, divulgación o uso fraudulento, de obligado cumplimiento para los usuarios que intervienen en el tratamiento de los datos.

8. Principio de Confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley 1581 de 2012 y en los términos de la misma.

4. AUTORIZACIÓN USO DE DATOS PERSONALES

La autorización del Titular será requerida con antelación y/o al momento de realizar cualquier tratamiento de datos personales según el artículo 9 de la Ley 1581 de 2012. Esta autorización se obtendrá de manera expresa, a través de medios digitales, electrónicos, escritos u orales o cualquier otro medio que garantice su autenticidad, permita conservar prueba de la autorización y/o de la conducta inequívoca descrita en el artículo 2.2.2.25.2.2. sección 2 del capítulo 25 del Decreto 1074 de 2015. Visum TIC Group S.A.S, solicitará al Titular del dato su autorización para efectuar recolección, almacenamiento, uso, circulación y eliminación de los datos personales, indicando la finalidad para la cual se solicitan.

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

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

4.1 Solicitud de autorización al titular del dato personal

La autorización para el uso y/o tratamiento de los datos será gestionada por Visum TIC Group S.A.S, a través de mecanismos que garanticen su consulta posterior y la manifestación de la voluntad del Titular a través de los siguientes medios:

- Por escrito.
- De forma oral.
- Mediante canales automatizados.
- Mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización.

Visum TIC Group S.A.S, con antelación y/o al momento de efectuar la recolección del dato personal, informará de manera clara y expresa al Titular, 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 (NOMBRE DE LA EMPRESA).

4.2 Autorización y tratamiento de datos sensibles

En los casos en los cuales se requiere el tratamiento de datos sensibles se informará al Titular el carácter facultativo de su aprobación y suministro, sólo serán tratados con su aprobación indicando los fines para los cuales son recolectados. En general se prohíbe el tratamiento de datos sensibles, excepto cuando:

1. El titular haya dado su autorización explícita para dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.
2. El Tratamiento sea necesario para salvaguardar el interés vital del titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
3. El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
4. El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

4.2.2 Tratamiento de datos biométricos

La recolección de datos biométricos (huellas dactilares, imágenes faciales, iris, RH, entre otros), se realizará solo cuando sea estrictamente necesario y con la debida justificación para alcanzar los fines establecidos con el fin de garantizar el cumplimiento de las leyes de protección de datos personales y proteger la privacidad de los titulares de los datos. El titular de los datos será informado de manera clara y comprensible sobre el tipo de datos biométricos que se recogerán, el propósito de la recolección, el plazo de conservación, así como sus derechos en relación con dichos datos.

4.3 Autorización y tratamiento de datos de menores de edad

Visum TIC Group S.A.S de acuerdo con el artículo 7° de la Ley 1581 de 2012, realizará Tratamiento de datos personales de niños, niñas y adolescentes en el marco de los criterios señalados en el artículo 2.2.2.25.2.9 sección 2 del capítulo 25 del Decreto 1074 de 2015 (Artículo 12 del Decreto 1377 de 2013), con observancia de los siguientes parámetros y requisitos:

1. Que el uso del dato responda y respete el interés superior de los niños, niñas y adolescentes.
2. Que en el uso del dato se asegure el respeto de sus derechos fundamentales del menor.

La autorización para el tratamiento de datos de menores de edad será solicitada al representante legal del niño, niña o adolescente previo ejercicio del menor de su derecho a ser escuchado, opinión que

será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto. En calidad de Responsable y/o Encargado velará por el uso adecuado de los datos de niños, niñas y adolescentes aplicando los principios y obligaciones establecidos en la Ley 1581 de 2012 y normas reglamentarias. Asimismo, identificará los datos sensibles recolectados o almacenados con el fin de incrementar la seguridad y tratamiento de la información.

5. TRATAMIENTO Y FINALIDADES DE LAS BASES DE DATOS

Visum TIC Group S.A.S, como responsable del tratamiento de los datos personales contenidos en sus bases de datos y/o archivos que gestiona, realizará tratamiento el cual comprenderá la recolección, almacenamiento, uso, circulación y eliminación, a través de medios físicos o digitales. El Tratamiento solo se realizará para fines específicos, legítimos y previamente informados al Titular, cumpliendo con la Constitución y la Ley. Las finalidades del tratamiento de cada una de las bases de datos podrán ser consultadas en el Anexo 1. Finalidades de bases de datos, el cual hace parte integral de la presente política.

5.1 Registro Nacional de Bases de datos – RNBD

Visum TIC Group SAS, contará con un inventario de bases de datos en el cual se incorpore la información que deberá ser inscrita en el RNBD y velará por las correspondientes actualizaciones. De conformidad con el artículo 25 de la Ley 1581 y sus decretos reglamentarios, registrará sus bases de datos junto con la presente política de tratamiento de Datos Personales, en el Registro Nacional de bases de datos administrado por la Superintendencia de Industria y Comercio, de conformidad con el procedimiento establecido para el efecto.

6. TRATAMIENTO DE DATOS EN LOS SISTEMAS DE VIDEOVIGILANCIA:

Visum TIC Group SAS, realiza monitoreo y observación de las instalaciones físicas de la sociedad a través de los sistemas de videovigilancia o cámaras de seguridad, en los cuales se recolectan imágenes de personas. Por tratarse de datos de carácter sensible según el artículo 5 de la ley 1581 de 2012, se informará a los Titulares de los datos mediante la fijación de anuncios instalados en las áreas de acceso a los lugares que están siendo vigilados y monitoreados, quién es el Responsable del Tratamiento, las finalidades del tratamiento, los derechos del Titular, los canales habilitados para ejercer los derechos del Titular, así como, dónde se encuentra publicada la Política de Tratamiento de la Información, cumpliendo con los parámetros establecidos en la Guía para la Protección de Datos Personales en Sistemas de Videovigilancia, expedidos por la SIC como autoridad de control. Las imágenes deberán ser conservadas por un tiempo máximo de 60 días.

En los casos en los cuales la imagen sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, su conservación se extenderá por el periodo necesario hasta que sea resuelto el caso.

7. DERECHOS DE LOS TITULARES

Visum TIC Group SAS, garantizará el ejercicio de derechos de los Titulares de los datos en relación con su tratamiento según la normatividad vigente, los siguientes:

7.1 Derecho de acceso o consulta:

Se trata del derecho del Titular a ser informado por el responsable del tratamiento, previa solicitud, respecto al origen, uso y finalidad que les han dado a sus datos personales.

***7.2** Derechos de quejas y reclamos:*

La Ley distingue cuatro tipos de reclamos:

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

7.3 *Personas legitimadas para el ejercicio de los derechos de titulares de datos personales*.

Estos derechos podrán ser ejercidos por las siguientes personas:

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

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

7.4 Derecho a solicitar prueba de la autorización otorgada al Responsable del tratamiento

Salvo cuando expresamente se exceptúe como requisito para el tratamiento de conformidad con lo previsto en el artículo 10 de la LEPD.

7.5 Derecho a presentar ante la Superintendencia de Industria y Comercio quejas por infracciones

El Titular tiene el derecho de presentar quejas ante la autoridad competente si considera que sus derechos han sido vulnerados.

8 PROCEDIMIENTO ATENCIÓN A TITULARES

8.1 Atención a los titulares de datos

Visum TIC Group SAS, ha designado un responsable de la gestión y atención de las peticiones, consultas y reclamos que los titulares de los datos personales puedan presentar. Los titulares pueden enviar sus solicitudes a través de los siguientes canales de comunicación:

- **Correo electrónico**: info@visumtic.com
- **Dirección postal**: Calle 26A No. 13 97. Oficina 1501. Edificio Bulevar Tequendama. Centro Internacional

8.2 Procedimientos para ejercer los derechos del titular

Los titulares de los datos tienen derecho a acceder, consultar, y presentar reclamos sobre sus datos personales. A continuación, se describe el procedimiento para el ejercicio de estos derechos:

8.2.1 Derecho de acceso o consulta

El responsable de la gestión y atención de las peticiones, consultas y reclamos garantizará al titular el derecho de consultar sus datos personales en los términos, plazos y condiciones establecidos en la Ley 1581 de 2012 y en las presentes políticas. Las consultas deberán contener como mínimo la siguiente información:

- Nombre y apellidos del titular.
- Fotocopia de la cédula de ciudadanía del titular y, si aplica, del representante legal.
- Petición detallada de la consulta o acceso solicitado.
- Dirección de notificación, fecha y firma del solicitante.
- Documentos adicionales que respalden la solicitud, si corresponde.

8.2.2 **Plazos para la resolución de consultas**

Una vez recibida la solicitud, se resolverá la consulta en un plazo máximo de diez (10) días hábiles. En caso de no poder atender la consulta dentro de ese plazo, se informará al interesado sobre el motivo de la demora y se proporcionará una nueva fecha de respuesta, que no podrá exceder cinco (5) días hábiles adicionales.

8.3 Derechos de quejas y reclamos

El titular de los datos tiene derecho a presentar reclamos respecto a sus datos personales, tales como: solicitar la corrección, supresión, revocación de autorización o en caso de alguna infracción. El responsable de la gestión y atención de las peticiones, consultas y reclamos garantizará al titular dará trámite en los términos, plazos y condiciones establecidos en la Ley 1581 de 2012 y en las presentes políticas. Las reclamaciones presentadas deberán contener como mínimo la siguiente información:

- Nombre y apellidos del titular.
- Fotocopia de la cédula de ciudadanía del titular y, si aplica, del representante legal.

- Descripción de los hechos y petición concreta relacionada con la solicitud de corrección, supresión, revocación o infracción.
- Dirección de notificación, fecha y firma del solicitante.
- Documentos adicionales que respalden la solicitud, si corresponde.

Si el reclamo está incompleto, se requerirá al interesado dentro de los cinco (5) días hábiles siguientes a la recepción del reclamo para que subsane las omisiones. Si transcurridos dos (2) meses desde la fecha del requerimiento no se presenta la información requerida, se entenderá que el reclamo ha sido desistido. Una vez recibido el reclamo completo, se registrará una leyenda en la base de datos indicando que el "reclamo está en trámite", junto con el motivo del reclamo. Esta leyenda deberá mantenerse hasta que el reclamo sea resuelto.

Cuando se solicitare la supresión de datos y/o la revocatoria de la autorización de datos personales no procederá cuando el Titular tenga un deber legal o contractual de permanecer en la base de datos.

8.3.1 Plazos para la resolución de reclamos

El responsable de la gestión y atención de las peticiones, consultas y reclamos resolverá el reclamo dentro de un plazo máximo de quince (15) días hábiles desde la fecha de recepción de la solicitud. Si no es posible atender el reclamo dentro de este plazo, se informará al interesado sobre los motivos de la demora y la nueva fecha estimada de resolución, la cual no podrá superar los ocho (8) días hábiles siguientes al vencimiento del plazo original.

9. DEBERES DEL RESPONSABLE DEL TRATAMIENTO.

Visum TIC Group SAS, como responsable del tratamiento, debe cumplir con los deberes establecidos por el artículo 17 de Ley 1581 de 2012, sin perjuicio de las demás disposiciones previstas en la ley y aquellas que la modifiquen, adicionen o sustituyan, entre otros, los siguientes:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
b) Solicitar y conservar, en las condiciones previstas en la ley, copia de la respectiva autorización otorgada por el Titular.
c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.
g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.
h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la ley.

i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
j) Tramitar las consultas y reclamos formulados en los términos señalados en la ley.
k) Adoptar procedimientos específicos para garantizar el adecuado cumplimiento de la ley y en especial, para la atención de consultas y reclamos.
l) 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.
m) 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.

10. DEBERES DEL ENCARGADO DEL TRATAMIENTO

Visum TIC Group SAS, podrá actuar como encargado del tratamiento de datos personales, en estos casos, deberá cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la ley y en los acuerdos entre Responsable y Encargado:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la Ley 1581 de 2012 y demás normas concordantes y vigentes.
d) Actualizar la información reportada por los responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.
e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente política.
f) Adoptar un Manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares.
g) Registrar en las bases de datos la leyenda "reclamo en trámite" en la forma en que se regula en la ley.
h) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.
m) Verificar que el responsable del Tratamiento tiene la autorización para el tratamiento de datos personales del Titular.

11. MEDIDAS DE SEGURIDAD

Visum TIC Group SAS, implementará medidas organizativas, humanas y técnicas para garantizar la seguridad de los datos personales, evitando su acceso no autorizado, pérdida o divulgación indebida. Estas medidas serán esenciales para proteger la confidencialidad, integridad y disponibilidad de la información, lo que reduce el riesgo de filtraciones de datos, pérdidas financieras, daños a la reputación y sanciones regulatorias. La implementación adecuada de estas medidas no solo mejora la seguridad, sino que también garantiza el cumplimiento del principio de seguridad consagrado en el artículo 4 literal g) de la Ley 1581 de 2012 y otras normativas de protección de datos, así como, estándares internacionales, fortaleciendo la confianza de todas los clientes, aliados, usuarios y titulares de datos.

Para implementar las medidas de seguridad necesarias para garantizar la confidencialidad**,** integridad y disponibilidad de la información, se deberán aplicar las directrices contenidas en la Política Interna de Seguridad de la Información de la sociedad en todas las áreas y/o procesos en los cuales se realiza tratamiento de datos personales.

12. POLÍTICA DE COOKIES

Visum TIC Group SAS, utiliza cookies y tecnologías similares en su sitio web www.visumtic.com para mejorar la experiencia de usuario y garantizar el funcionamiento adecuado del mismo. Al utilizar nuestro sitio web, usted acepta el uso de cookies de acuerdo con esta política. Si no está de acuerdo con el uso de cookies, le recomendamos que ajuste la configuración de su navegador o que se abstenga de utilizar nuestro sitio.

Las cookies son pequeños archivos de texto que se almacenan en el dispositivo (ordenador, smartphone, tablet) cuando usted visita un sitio web. Estas cookies permiten que el sitio recuerde sus acciones y preferencias (como el idioma, el tamaño de la fuente y otras configuraciones de visualización) durante un periodo de tiempo, para que no tenga que volver a configurarlas cada vez que regrese al sitio o navegue de una página a otra. Nuestro sitio web utiliza los siguientes tipos de cookies:

Cookies Necesarias: Son esenciales para que el sitio web funcione correctamente y permitan la navegación por el sitio y la utilización de sus funciones, como el acceso a áreas seguras. Sin estas cookies, no podríamos proporcionar los servicios solicitados por el usuario.

Cookies de Rendimiento: Recogen información sobre cómo los usuarios interactúan con nuestro sitio web, por ejemplo, las páginas que visitan con más frecuencia y si reciben mensajes de error. Estas cookies no recopilan información que identifique a un usuario y se utilizan únicamente para mejorar el rendimiento del sitio.

Cookies de Funcionalidad: Permiten al sitio web recordar las elecciones que hace el usuario (como el idioma o la región) y proporcionar características personalizadas. Estas cookies mejoran la experiencia de usuario, pero no son esenciales para el funcionamiento básico del sitio.

Cookies de Publicidad y Marketing: Se utilizan para ofrecer anuncios más relevantes para el usuario, basados en sus intereses. También se utilizan para limitar el número de veces que se muestra un anuncio y medir la efectividad de las campañas publicitarias.

Cookies de Terceros: Nuestro sitio web también puede utilizar cookies de terceros (por ejemplo, Google Analytics, redes sociales, servicios de publicidad) para recopilar información sobre su uso del sitio y mejorar los servicios proporcionados.

Usted puede gestionar las cookies a través de la configuración de su navegador. La mayoría de los navegadores permiten controlar las cookies mediante sus configuraciones de privacidad, donde puede optar por aceptar, bloquear o eliminar cookies. Sin embargo, si decide desactivar las cookies, algunas características de nuestro sitio web pueden no funcionar correctamente. Para obtener más información sobre cómo configurar las cookies en los navegadores más comunes, consulte los siguientes enlaces:

Google Chrome: [Configuración de cookies en Chrome]
Mozilla Firefox: [Configuración de cookies en Firefox]
Microsoft Edge: [Configuración de cookies en Edge]
Safari: [Configuración de cookies en Safari]

Nos reservamos el derecho de modificar esta Política de Cookies en cualquier momento. Cualquier cambio será publicado en esta página con la fecha de la última actualización. Le recomendamos que consulte regularmente esta política para estar informado sobre cómo utilizamos las cookies.

13. PROCEDIMIENTO GESTIÓN Y REPORTE ANTE INCIDENTES DE SEGURIDAD

Visum TIC Group SAS, contará con un procedimiento interno para la gestión y reporte ante cualquier incidente de seguridad relacionado con los datos personales. Se entiende por incidente de seguridad cualquier evento o actividad que compromete la confidencialidad, integridad o disponibilidad de la información o los sistemas de una organización, que pueden ser causados por fallos técnicos, errores humanos o acciones maliciosas. Los incidentes de seguridad pueden involucrar el acceso no autorizado a datos, pérdida de información, interrupciones en los servicios o la exposición de datos personales o confidenciales.

Tipos comunes de incidentes de seguridad incluyen:

- Ciberataques: Como los ataques de ransomware, phishing, malware, o ataques de denegación de servicio (DDoS).
- Accesos no autorizados: Intentos de acceder o robar información por personas no autorizadas.
- Pérdida de datos: Incluye la pérdida, robo o destrucción accidental de información valiosa.
- Filtraciones de información: Exposición no autorizada de datos confidenciales, como la divulgación pública de datos personales o financieros.
- Errores humanos: Actividades incorrectas o negligentes realizadas por empleados que resultan en la vulneración de la seguridad.

Cuando se presente un incidente de seguridad el Oficial de Protección de Datos, será el encargado de coordinar la gestión de atención, respuesta y del respectivo reporte ante la Superintendencia de Industria y Comercio siguiendo las directrices señaladas en el procedimiento interno para el efecto. Los usuarios y responsables de procedimientos, así como cualquier persona que tenga relación con

el almacenamiento, tratamiento o consulta de las bases de datos recogidas en este documento, deben conocer el procedimiento para actuar en caso de incidencia.

El procedimiento de gestión y reporte ante incidentes es el siguiente:

1. Identificación y evaluación del Incidente

Detección: El primer paso es identificar de manera inmediata el incidente de seguridad. Este puede ser reportado por cualquier empleado o detectado a través de herramientas de monitoreo.

Evaluación Inicial: El responsable de seguridad de la información debe realizar una evaluación preliminar para determinar la naturaleza, alcance y gravedad del incidente. Esto incluye identificar si ha habido acceso no autorizado a datos personales, alteración, pérdida o destrucción de la información.

2. Contención y Mitigación

Acciones Inmediatas: Se deberán tomar medidas para contener el incidente y mitigar su impacto. Esto puede incluir la desconexión de sistemas afectados, la revocación de accesos no autorizados, o la implementación de medidas adicionales de seguridad.

Preservación de Evidencias: Se procederá con la preservación de toda la información relacionada con el incidente para facilitar la investigación y posible auditoría futura. Esto incluye logs, registros de acceso y otros datos relevantes.

3. Notificación Interna

El incidente deberá ser reportado de inmediato al Comité de Seguridad de la Información y al Oficial de Protección de datos personales, según los procedimientos internos establecidos.

4. Análisis y Reporte a la SIC

Análisis del Impacto: Se deberá realizar una evaluación de impacto en la cual se pueda determinar si el incidente afecta a datos personales y evaluar su riesgo sobre los derechos y libertades de los titulares de la información, así como, afectaciones a económicas y reputacionales a la sociedad y a terceros.

Reporte a la SIC: Si el incidente implica afectación a los derechos de los titulares de los datos personales, se debe notificar y/o reportar a la Superintendencia de Industria y Comercio (SIC) en un plazo máximo de 15 días calendario a partir de la detección del incidente. El reporte debe enviarse a través de los canales oficiales establecidos por la SIC, según se indique en la normativa vigente.

5. Comunicación a los Titulares Afectados

Si el incidente implica un alto riesgo para los derechos de los titulares, se procederá con la notificación informándoles la naturaleza del incidente, los posibles efectos y las medidas correctivas adoptadas.

6. Investigación y Resolución

Investigación Interna: Iniciar una investigación interna para determinar las causas del incidente y establecer acciones correctivas y preventivas para evitar futuros eventos similares.

Informe Final: Elaborar un informe detallado sobre la investigación y los pasos tomados para resolver el incidente, el cual debe ser archivado y disponible para auditorías futuras.

7. Seguimiento y Mejora Continua

Se deberán revisar y actualizar los procedimientos de seguridad, políticas y controles internos para prevenir que se presenten incidentes similares.

14. ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE LOS DATOS

Visum TIC Group SAS, implementará mecanismos para la identificación, evaluación y mitigación de los riesgos asociados con el tratamiento de datos personales. La administración de riesgos asociados al tratamiento de los datos es un proceso clave dentro de la gestión de la seguridad de la información y la protección de datos personales y tiene como objetivo identificar, evaluar y mitigar los riesgos que pueden surgir durante el manejo de los datos, asegurando que se cumplan las normas aplicables y los principios de confidencialidad**,** integridad y disponibilidad de los datos personales que procesa la sociedad.

15. ENTREGA DE DATOS PERSONALES A LAS AUTORIDADES

Los datos personales podrán ser entregados a las autoridades competentes en los casos establecidos por la ley, garantizando la seguridad y protección de la información. La entrega de datos personales a entidades administrativas y judiciales debe realizarse siempre de manera legal**,** transparente y proporcionada, asegurando que el requerimiento esté justificado y que se tomen todas las medidas necesarias para proteger los derechos de los titulares de los datos de acuerdo con los criterios señalados en la Ley 1581 de 2012. Para la entrega de datos personales a las entidades administrativas o judiciales se deberá tener en cuenta el siguiente proceso, el cual deberá constar en un acta que garantice la trazabilidad y seguridad de la información que será suministrada:

- **Verificación de la solicitud**: Antes de entregar cualquier dato personal, la organización se verificará que el requerimiento proviene de una autoridad competente, que esté debidamente autorizado por la ley, y que cumpla con los requisitos formales establecidos (como la presentación de una orden judicial o un requerimiento administrativo formal).
- **Consentimiento del titular**: En ciertas situaciones el consentimiento del titular no será necesario por mandato legal, sin embrago, se recomienda informar al titular de los datos sobre la solicitud, salvo que de esta manera se interfiera con la investigación en curso.
- **Entrega de los datos**: La información debe ser entregada de manera segura y limitada a lo estrictamente necesario para cumplir con el requerimiento. Se deben utilizar métodos que garanticen la confidencialidad e integridad de los datos, como la transmisión cifrada o el uso de medios seguros para la entrega.

- **Registro y documentación**: La organización debe mantener un registro detallado de la solicitud, la entrega de los datos y cualquier otra acción tomada en relación con el requerimiento. Esto incluye la fecha de la solicitud, el contenido solicitado (datos suministrados), la identidad del solicitante, y cualquier comunicación relacionada con el proceso.

16. TRANSFERENCIA Y TRANSMISIÓN INTERNACIONAL DE DATOS PERSONALES

Visum TIC Group SAS, en caso de realizar transferencia y transmisión internacional de datos personales en cumplimiento de la Ley 1581 de 2012 y con el fin de proteger los derechos de los titulares de los datos, seguirá las siguientes directrices:

1. Evaluación previa del país receptor: Verificar si el país receptor garantiza un nivel adecuado de protección de datos personales, la Superintendencia de Industria y Comercio (SIC) ha identificado algunos países que considera ofrecen garantías suficientes de protección. Si el país receptor no se encuentra en este listado, la transferencia de datos solo podrá realizarse con aprobación de la SIC, mediante una Declaración de Conformidad.

2. Obtención del consentimiento del Titular: Si el Titular de los datos personales no el otorgado consentimiento previo, expreso e informado no se podrá realizar la transferencia internacional de datos. Salvo las excepciones contempladas en la ley.

3. Implementación norma corporativa vinculante: Si el país receptor no asegura un nivel adecuado de protección de datos personales, pero se encuentra aprobada una Norma Corporativa Vinculante en la cual se incluye al Responsable de tratamiento receptor de los datos personales, podrá realizarse la transferencia asegurando que entre entidades del mismo grupo cumplan con las mismas garantías de protección.

4. Documentación y registro de la transferencia: La transferencia de datos personales deberá documentarse de la siguiente manera:

- La base legal que justifica la transferencia (consentimiento, contrato, obligación legal, etc.).
- La descripción de las medidas de protección aplicadas a los datos durante la transferencia.
- El acuerdo firmado con el receptor (si corresponde) y las cláusulas de protección implementadas.

El Oficial de Protección de Datos deberá registrar las transferencias internacionales de datos e informar a las auditorías internas o externas sobre sus condiciones, dicho registro deberá estar disponible en caso de ser requerido por la SIC.

5. Supervisión: El Oficial de Protección de Datos deberá implementar un plan de monitoreo para verificar el cumplimiento de las directrices de transferencia y transmisión internacional de datos, incluyendo auditorías periódicas para asegurar que los datos se estén manejando de acuerdo con las garantías estipuladas, supervisar el cumplimiento de las condiciones pactadas en entidades receptoras y una revisión periódica del marco normativo en el país receptor y su conformidad con las leyes colombianas de protección de datos.

17. PERÍODO DE VIGENCIA DE LAS BASES DE DATOS

Las bases de datos responsabilidad de Visum TIC Group SAS, serán objeto de tratamiento durante el tiempo que sea razonable y necesario para la finalidad para la cual son recabados los datos y de acuerdo con la autorización otorgada por los Titulares de los datos personales, así como, las normas especiales que regulen la materia y las directrices que establezca la SIC en el ejercicio de las funciones legales asignadas.

18. VIGENCIA

La presente política empieza a regir a partir de la fecha de su aprobación y se mantendrá vigente hasta su actualización o modificación conforme a la legislación aplicable. Cualquier cambio sustancial en las políticas de Tratamiento de datos personales, se comunicará de forma oportuna a los titulares de los datos a través de los medios habituales de contacto y/o a través de su sitio web.

19. ANEXOS.

Anexo 1. Finalidades de bases de datos

Anexo 2. Procedimiento gestión y reporte de incidentes de seguridad

20. HISTÓRICO DE APROBACIONES Y ACTUALIZACIONES

Versión 1.0: 06 de diciembre de 2024

Aprobación: 06 de diciembre de 2024