1. BASE LEGAL Y ÁMBITO DE APLICACIÓN 3

1.1. Alcance 3

1.2. Normatividad Aplicable 3

2. DEFINICIONES 4

3. PRINCIPIOS DE LA PROTECCIÓN DE DATOS 7

3.1. Principio de Legalidad: 7

3.2. Principio de Finalidad: 7

3.3. Principio de Libertad 8

3.4. Principio de veracidad o Calidad 8

3.5. Principio de Transparencia 8

3.6. Principio de acceso y circulación Restringida 8

3.7. Principio de Seguridad 9

3.8. Principio de confidencialidad 9

4. AUTORIZACIÓN DE LA POLÍTICA DE TRATAMIENTO 9

5. RESPONSABLE DEL TRATAMIENTO 10

6. TRATAMIENTO Y FINALIDADES DE LAS BASES DE DATOS 10

7. DERECHOS DE LOS TITULARES 11

7.1. Derecho de acceso o consulta 12

7.2. Derechos de quejas y reclamos 12

8. SOLICITUD DE AUTORIZACIÓN AL TITULAR DEL DATO PERSONAL 13

9. TRATAMIENTO DE DATOS DE MENORES 13

10. ATENCIÓN A LOS TITULARES DE DATOS 14

11. PROCEDIMIENTOS PARA EJERCER LOS DERECHOS DEL TITULAR 14

11.1. Derecho de acceso o consulta 14

11.2. Derechos de quejas y reclamos 16

12. MEDIDAS DE SEGURIDAD 17

13. PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENCIAS 20

14. ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE LOS DATOS 22

15. ENTREGA DE DATOS PERSONALES A LAS AUTORIDADES 23

16. TRANSFERENCIA DE DATOS A TERCEROS PAÍSES 23

17. TRATAMIENTO DE DATOS BIOMÉTRICOS 24

18. REGISTRO NACIONAL DE BASES DE DATOS - RNBD 25

19. SEGURIDAD DE LA INFORMACIÓN Y DATOS PERSONALES 25

20. GESTIÓN DE DOCUMENTOS 26

1. BASE LEGAL Y ÁMBITO DE APLICACIÓN

La política de tratamiento de la información se desarrolla en cumplimiento del Artículo 15 de la Constitución Política; de los artículos 17 literal k) y 18 literal f) de la Ley Estatutaria 1581 de 2012 por la cual se dictan disposiciones generales para la Protección de Datos Personales (LEPD); del artículo 2.2 .2.25.1.1 sección 1 capítulo 25 del Decreto 1074 de 2015, por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Esta política será aplicable a todos los datos personales registrados en bases de datos que sean objeto de tratamiento por el responsable del tratamiento.

1.1. Alcance

El presente documento aplicará para todos aquellos datos personales o de cualquier otro tipo de información que sea utilizada o repose en las bases de datos y archivos de TODODROGAS CIA S.A.S., respetando los criterios para la obtención, recolección, uso, tratamiento, procesamiento, intercambio, transferencia y transmisión de datos personales, y fijar las responsabilidades de TODODROGAS CIA S.A.S. y de sus empleados en el manejo y tratamiento de los datos personales que reposen en sus bases de datos y archivos, información la cual, podrá dar tratamiento tanto directamente como por terceros aliados, legalmente delegados para tal fin (encargado del tratamiento).

1.2. Normatividad Aplicable

- Constitución Política de Colombia
- Ley 1581 de 2012

- Decreto 1074 de 2015 Capitulo 25 y Capitulo 26 compilatorios de los decretos:
- Decreto 1377 de 2013
- Decreto 886 de 2014
- Circulares externas e instrucciones impartidas por la Superintendencia de Industria y Comercio, en especial la Circular Externa 01 de 2016.

2. DEFINICIONES Y ABREVIATURAS

Las siguientes definiciones se encuentran establecidas en el artículo 3 de la LEPD y artículo 2.2.2.25.1.3 sección 1 Capitulo 25 del decreto 1074 de 2015 (Artículo 3 del decreto 1377 de 2013).

Autorización	Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.
Base de Datos	Conjunto organizado de datos personales que sea objeto de tratamiento.
Dato Personal	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
Dato 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 del servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales, sentencias judiciales debidamente ejecuto- riadas que no estén sometidas a reserva.

Dato Semiprivado	Es aquel que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como son: Bases de datos que contengan Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.
Dato Privado	Es un dato personal que por su naturaleza íntima o reservada solo interesa a su titular y para su tratamiento requiere de su autorización previa, informada y expresa. Bases de datos que contengan datos como números telefónicos y correos electrónicos personales; datos laborales, sobre infracciones administrativas o penales, administrados por administraciones tributarias, entidades financieras y entidades gestoras y servicios comunes de la Seguridad Social, bases de datos sobre solvencia patrimonial o de crédito, bases de datos con información suficiente para evaluar la personalidad del titular, bases de datos de los responsables de operadores que presten servicios de comunicación electrónica.
Dato Sensible	Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la 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.

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.
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.
Responsable de Administrar las Bases de Datos	Empleado encargado de controlar y coordinar la adecuada aplicación de las políticas del tratamiento de los datos una vez almacenados en una base datos especifica; así como de poner en práctica las directrices que dicte el Responsable del tratamiento y el Oficial de Protección de datos.
Oficial de Protección de Datos	Es la persona natural que asume la función de coordinar la implementación del marco legal en protección de datos personales, que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012.
Titular	Persona natural cuyos datos personales sean objeto de tratamiento.
Tratamiento	Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
Aviso de Privacidad	Comunicación verbal o escrita generada por el Responsable, 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 información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

Transferencia	La transferencia de datos tiene lugar cuando el Responsable y/o Encargado 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	Tratamiento de datos personales que implica la comunicación de los mismos 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.

3. PRINCIPIOS DE LA PROTECCIÓN DE DATOS

El artículo 4 de la LEPD establece unos principios para el tratamiento de datos personales que se han de aplicar, de manera armónica e integral, en el desarrollo, interpretación y aplicación de la Ley.

Los principios legales de la protección de datos son los siguientes:

3.1. Principio de Legalidad:

El tratamiento de los datos es una actividad reglada que debe sujetarse a lo establecido en la LEPD, el Decreto 1377 de 2013 Compilado en el Capítulo 25 del Decreto 1074 de 2015 y en las demás disposiciones que la desarrollen.

3.2. Principio de Finalidad:

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

3.3. Principio de Libertad

El tratamiento solo puede ejercerse con el consentimiento previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que revele el consentimiento. El tratamiento de los datos requiere la autorización previa e informada del Titular por cualquier medio que permita ser consultado con posterioridad.

3.4. Principio de veracidad o Calidad

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

3.5. Principio de Transparencia

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

3.6. 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 LEPD y la Constitución. En este sentido, el tratamiento solo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la Ley. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet y otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los Titulares o terceros autorizados conforme a la Ley.

3.7. Principio de Seguridad

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

3.8. 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 solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la LEPD y en los términos de la misma.

4. AUTORIZACIÓN DE LA POLÍTICA DE TRATAMIENTO

De acuerdo al artículo 9 de la LEPD, para el tratamiento de datos personales se requiere la autorización previa e informada del Titular. Mediante la aceptación de la presente política, todo Titular que facilite información relativa a sus datos

personales está consintiendo el tratamiento de sus datos por parte de TODODROGAS CIA S.A.S., en los términos y condiciones recogidos en la misma.

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

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

5. RESPONSABLE DEL TRATAMIENTO

El responsable del tratamiento de las bases de datos objeto de esta política es TODODROGAS CIA S.A.S., cuyos datos de contacto son los siguientes:

- Dirección: Calle 50 # 48 03 Piso 2, Medellín, Antioquia.
- Correo electrónico: protecciondatos@tododrogas.com.co
- Teléfono: 6043222432

6. TRATAMIENTO Y FINALIDADES DE LAS BASES DE DATOS

TODODROGAS CIA S.A.S., en el desarrollo de su actividad empresarial, institucional y de distribución, realiza el tratamiento de datos personales de personas naturales y jurídicas vinculadas a sus operaciones, incluidos, entre otros, usuarios del sistema de salud, clientes institucionales, clientes del canal de distribución, proveedores, aliados estratégicos, contratistas, empleados y autoridades, para el cumplimiento de finalidades legítimas, conforme a la Constitución Política y la ley, tales como:

- Gestionar la prestación del servicio de dispensación y entrega de tecnologías en salud a los usuarios autorizados por las entidades responsables del aseguramiento en salud.
- Ejecutar y administrar las relaciones contractuales con clientes institucionales, entidades del sistema de salud, clínicas, hospitales, IPS, proveedores y aliados.
- Cumplir con obligaciones legales, regulatorias, sanitarias, contables, tributarias y administrativas.
- Gestionar peticiones, quejas, reclamos, solicitudes, denuncias y requerimientos presentados por titulares de la información o por autoridades competentes.
- Adelantar procesos de facturación, auditoría, conciliación, cartera y soporte operativo derivados de las relaciones contractuales.
- Realizar análisis internos, estadísticas operativas y reportes institucionales, necesarios para la adecuada gestión de los procesos de la sociedad.
- Garantizar la seguridad de la información, la prevención del fraude, la mitigación de riesgos operativos y el cumplimiento de los estándares de control interno.
- Compartir información con aliados, encargados del tratamiento y terceros autorizados, cuando sea necesario para el desarrollo de las actividades propias de la sociedad, siempre bajo los principios y garantías de la Ley 1581 de 2012.
- Atender requerimientos de autoridades administrativas y judiciales, en ejercicio de sus funciones legales.

En todo caso, el tratamiento de los datos personales se realizará exclusivamente para fines institucionales, contractuales, operativos y legales, y dentro del marco de las autorizaciones otorgadas por los titulares y la normativa vigente.

7. DERECHOS DE LOS TITULARES

De acuerdo con el artículo 8 de la LEPD, articulo 2.2.2.25.4.1 sección 4 capítulo 25 del Decreto 1074 de 2015 (Artículos 21 y 22 del Decreto 1377 de 2013), los Titulares

de los datos pueden ejercer una serie de derechos en relación al tratamiento de sus datos personales. Estos derechos podrán ejercerse por las siguientes personas.

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

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

Los derechos del Titular son los siguientes:

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. 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.

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

El Titular o causahabiente solo podrá elevar ante la SIC – Superintendencia de Industria y Comercio la petición (queja), una vez haya agotado el trámite de consulta o reclamo ante el Responsable del tratamiento o Encargado del tratamiento.

8. SOLICITUD DE AUTORIZACIÓN AL TITULAR DEL DATO PERSONAL

Con antelación y/o al momento de efectuar la recolección del dato personal, TODODROGAS CIA S.A.S. solicitará al Titular del dato su autorización para efectuar su recolección y tratamiento, bien sea para dar tratamiento directo o por interpuesta persona legalmente delegada indicando la finalidad para la cual se solicita el dato, utilizando para esos efectos medios técnicos automatizados, escritos u orales, que permitan 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 (Artículo 7 del Decreto 1377 de 2013).

9. TRATAMIENTO DE DATOS DE MENORES

De acuerdo con el artículo 7° de la Ley 1581 de 2012, el Tratamiento de datos personales de niños, niñas y adolescentes está prohibido, salvo lo dispuesto 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) y en cumplimiento de los siguientes parámetros y requisitos:

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

Cumplidos los anteriores requisitos, TODODROGAS CIA S.A.S. solicitará al representante legal del niño, niña o adolescente la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto. El Responsable y Encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos, aplicando los principios y obligaciones establecidos en la Ley 1581 de 2012 y normas reglamentarias.

10. ATENCIÓN A LOS TITULARES DE DATOS

El Oficial de Protección de Datos de TODODROGAS CIA S.A.S. será el encargado de la atención de peticiones, consultas y reclamos ante la cual el Titular de los datos puede ejercer sus derechos. Teléfono: 3222432. Correo electrónico: protecciondatos@tododrogas.com.co.

11. PROCEDIMIENTOS PARA EJERCER LOS DERECHOS DEL TITULAR

11.1. Derecho de acceso o consulta

Según el artículo 2.2.2.25.4.2. sección 4 capítulo 25 del Decreto 1074 de 2015 (Artículo 21 del Decreto 1377 de 2013), el Titular podrá consultar de forma gratuita sus datos personales en dos casos:

- Al menos una vez cada mes calendario.
- Cada vez que existan modificaciones sustanciales de las políticas de tratamiento de la información que motiven nuevas consultas.

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

El Titular de los datos puede ejercitar el derecho de acceso o consulta de sus datos mediante un escrito dirigido a TODODROGAS CIA S.A.S. enviado, mediante correo electrónico a: protecciondatos@tododrogas.com.co , indicando en el Asunto "Ejercicio del derecho de acceso o consulta", o a través de correo postal remitido a Calle 50 # 48 03 Piso 2, MEDELLÍN, ANTIOQUIA.

La solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- Fotocopia de la Cédula de Ciudadanía del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Petición en que se concreta la solicitud de acceso o consulta.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada, cuando corresponda.
- El Titular podrá elegir una de las siguientes formas de consulta de la base de datos para recibir la información solicitada:
- Visualización en pantalla.
- Por escrito, con copia o fotocopia remitida por correo certificado o no.
- Correo electrónico u otro medio electrónico.
- Otro sistema adecuado a la configuración de la base de datos o a la naturaleza del tratamiento, ofrecido por TODODROGAS CIA S.A.S.

Una vez recibida la solicitud, TODODROGAS CIA S.A.S. resolverá la petición de consulta en un plazo máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma.

Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término. Estos plazos están fijados en el artículo 14 de la LEPD.
Una vez agotado el trámite de consulta, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

11.2. Derechos de quejas y reclamos

El Titular de los datos puede ejercitar los derechos de reclamo sobre sus datos mediante un escrito dirigido a TODODROGAS CIA S.A.S. enviado, mediante correo electrónico a protecciondatos@tododrogas.com.co , indicando en el Asunto "Ejercicio del derecho de acceso o consulta", o a través de correo postal remitido a Calle 50 # 48 03 Piso 2, MEDELLÍN, ANTIOQUIA.

La solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- Fotocopia de la Cédula de Ciudadanía del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Descripción de los hechos y petición en que se concreta la solicitud de corrección, supresión, revocación o infracción.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada que se quieran hacer valer, cuando corresponda.

Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

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

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

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

12. MEDIDAS DE SEGURIDAD

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

Por otra parte, TODODROGAS CIA S.A.S., mediante la suscripción de los correspondientes contratos de transmisión, ha requerido a los encargados del

tratamiento con los que trabaje la implementación de las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de la información en el tratamiento de los datos personales.

A continuación, se exponen las medidas de seguridad implantadas por TODODROGAS CIA S.A.S. (Tablas I y II).

TABLA I: Medidas de seguridad comunes para todo tipo de datos (públicos, semiprivados, privados, sensibles) y bases de datos (automatizadas, no automatizadas)				
Gestión de Documentos y Soportes	Control de Acceso	Incidencias	Personal	Manual Interno de Seguridad
1. Medidas que evidencien el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruidos.	1. Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones.	1. Registro de incidencias: tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras.	1. Definición de las funciones y obligaciones de los usuarios con acceso a los datos.	1. Elaboración e implementación del Manual de obligado cumplimiento para el personal.
2. Acceso restringido al lugar donde se almacenan los datos.	2. Lista actualizada de usuarios y accesos autorizados.	2. Procedimiento de notificación y gestión de incidencias.	2. Definición de las funciones de control y autorización delegadas por el responsable del tratamiento.	2. Contenido mínimo: ámbito de aplicación, medidas y procedimientos de seguridad, funciones y obligaciones del personal, descripción de las bases de datos,

TABLA I: Medidas de seguridad comunes para todo tipo de datos (públicos, semiprivados, privados, sensibles) y bases de datos (automatizadas, no automatizadas)				
Gestión de Documentos y Soportes	Control de Acceso	Incidencias	Personal	Manual Interno de Seguridad
				procedimiento ante incidencias, identificación de los encargados del tratamiento.
3. Autorización del responsable para la salida de documentos o soportes por medio físico o electrónico.	3. Mecanismos para evitar el acceso a datos con derechos distintos de los autorizados.		3. Divulgación entre el personal de las normas y consecuencias del incumplimiento de las mismas.	
4. Sistema de etiquetado o identificación del tipo de información.	4. Concesión, alteración o anulación de permisos por el personal autorizado.			
5. Inventario de soportes.				

TABLA II: Medidas de seguridad comunes para todo tipo de datos (públicos, semiprivados, privados, sensibles) según el tipo de bases de datos				
Base de Datos no Automatizadas			Base de Datos Automatizadas	
Archivo	Almacenamiento de Documentos	Custodia de Documentos	Identificación y Autenticación	Telecomunicaciones
1. Archivo de documentación siguiendo procedimientos que garanticen una correcta conservación, localización y consulta y permitan el ejercicio de los derechos de los titulares.	1. Dispositivos de almacenamiento con mecanismos que impiden el acceso a personas no autorizadas.	1. Deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de los mismos.	1. Identificación personalizada de usuarios para acceder a los sistemas de información y verificación de su autorización.	1. Elaboración e implementación del Manual de obligado cumplimiento para el personal.
			2. Mecanismos de identificación y autenticación; Contraseñas: asignación, caducidad y almacenamiento cifrado.	

13. PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENCIAS

TODODROGAS CIA S.A.S. establece un procedimiento de notificación, gestión y respuesta de incidencias con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información contenida en las bases de datos que están bajo su responsabilidad.

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 notificación, gestión y respuesta ante incidencias es el siguiente:

- Cuando una persona tenga conocimiento de una incidencia (perdida, hurto y/o acceso no autorizado) que afecte o pueda afectar la confidencialidad, disponibilidad e integridad de la información protegida de la empresa o alguno de los Encargados deberá comunicarlo, de manera inmediata, al Oficial de Protección de Datos, describiendo detalladamente el tipo de incidencia producida, e indicando las personas que hayan podido tener relación con la incidencia, la fecha y hora en que se ha producido, la persona que notifica la incidencia, la persona a quién se le comunica y los efectos que ha producido.
- Una vez comunicada la incidencia ha de solicitar al Oficial de Protección de Datos un acuse de recibo en el que conste la notificación de la incidencia con todos los requisitos enumerados anteriormente.
- TODODROGAS CIA S.A.S., crea un registro de incidencias que debe contener: el tipo de incidencia (Fraude Interno o externo, Daños a activos físicos, Fallas tecnológicas, Ejecución y administración de procesos), fecha y hora de la misma, persona que la notifica, persona a la que se le comunica, efectos de la incidencia y medidas correctoras cuando corresponda. Este registro es gestionado por el Oficial de Protección de Datos
- Asimismo, debe implementar los procedimientos para la recuperación de los datos cuando aplica, indicando quien ejecuta el proceso, los datos restaurados y, en su caso, los datos que han requerido ser grabados manualmente en el proceso de recuperación.
- Adicional, el Oficial de Protección de Datos debe informar a la Superintendencia de Industria y Comercio, mediante el RNBD dentro de los 15 días hábiles siguientes de haber sido detectado.

- Finalmente, TODODROGAS CIA S.A.S. notificará del incidente a los Titulares, cuando se identifique que puedan verse afectados de manera significativa.

14. ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE LOS DATOS

TODODROGAS CIA S.A.S., ha identificado riesgos relacionados con el tratamiento de los datos personales y establecidos controles con el fin de mitigar sus causas. Por ello, establecerá un sistema de gestión de riesgos junto con las herramientas, indicadores y recursos necesarios para su administración, cuando la estructura organizacional, los procesos y procedimientos internos, la cantidad de base datos y tipos de datos personales tratados por la organización se consideren que están expuestos a hechos o situaciones frecuentes o de alto impacto que incidan en la debida prestación del servicio o atenten contra la información de los titulares.

El sistema de gestión de riesgos determinará las fuentes tales como: tecnología, recurso humano, infraestructura y procesos que requieren protección, sus vulnerabilidades y las amenazas, con el fin de valorar su nivel de riesgo. Por lo que, para garantizar la protección de datos personales se tendrá en cuenta el tipo o grupo de personas internas y externas, los diferentes niveles de autorización de acceso. Asimismo, se observará la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial), tales como:

- Criminalidad: Entendida como las acciones, causadas por la intervención humana, que violan la ley y que están penalizadas por ésta.
- Sucesos de origen físico: Entendidos como los eventos naturales y técnicos, así como, los eventos indirectamente causados por la intervención humana.
- Negligencia y decisiones institucionales: Entendidos como las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema.

Al mismo tiempo son las amenazas menos predecibles porque están directamente relacionado con el comportamiento humano.

TODODROGAS CIA S.A.S. en el sistema de gestión de riesgo implementará las medidas de protección para evitar o minimizar los daños en caso de que se materialice una amenaza.

15. ENTREGA DE DATOS PERSONALES A LAS AUTORIDADES

Cuando por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial se soliciten a TODODROGAS CIA S.A.S. acceso y/o entrega de datos de carácter Personal contenidos en cualquiera de sus bases de datos, se verificará la legalidad de la petición, la pertinencia de los datos solicitados en relación con la finalidad expresada por la autoridad, y se suscribirá acta de la entrega de la información personal solicitada, precisando la obligación de garantizar los derechos del Titular, tanto al funcionario que hace la solicitud, a quien la recibe, así como a la entidad requirente.

16. TRANSFERENCIA DE DATOS A TERCEROS PAÍSES

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

- Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.
- Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del Titular por razones de salud o higiene pública.
- Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.
- Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.

- Transferencias necesarias para la ejecución de un contrato entre el Titular y el responsable del tratamiento o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.
- Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

Se debe tener en cuenta que, en los casos no contemplados como excepción, corresponderá a la Superintendencia de Industria y Comercio proferir la declaración de conformidad relativa a la transferencia internacional de datos personales.

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

17. TRATAMIENTO DE DATOS BIOMÉTRICOS

Los datos biométricos almacenados en las bases de datos son recolectados y tratados por motivos estrictamente de seguridad, para verificar la identidad personal y realizar control de acceso a los empleados, clientes y visitantes. Los mecanismos biométricos de identificación capturan, procesan y almacenan información relacionada con, entre otros, los rasgos físicos de las personas (las huellas dactilares, reconocimiento de voz y los aspectos faciales), para poder establecer o "autenticar" la identidad de cada sujeto.

La administración de las bases de datos biométrica se ejecuta con medidas de seguridad técnicas que garantizan el debido cumplimiento de los principios y las obligaciones derivadas de Ley Estatutaria en Protección de Datos asegurando además la confidencialidad y reserva de la información de los titulares.

18. REGISTRO NACIONAL DE BASES DE DATOS - RNBD

El término para registrar las bases de datos en el RNBD será el establecido legalmente.

Asimismo, los Responsables del Tratamiento deberán inscribir sus bases de datos en el Registro Nacional de Bases de Datos en la fecha en que la Superintendencia de Industria y Comercio habilite dicho registro, de acuerdo con las instrucciones que para el efecto imparta esa entidad. Las bases de Datos que se creen con posterioridad a ese plazo deberán inscribirse dentro de los dos (2) meses siguientes, contados a partir de su creación.

19. SEGURIDAD DE LA INFORMACIÓN Y DATOS PERSONALES

El cumplimiento del marco normativo en Protección de Datos Personales, la seguridad, reserva y/o confidencialidad de la información almacenada en las bases de datos es de vital importancia para TODODROGAS CIA S.A.S. Por ello, hemos establecido políticas, lineamientos y procedimientos y estándares de seguridad de la información, los cuales podrán cambiar en cualquier momento ajustándose a nuevas normas y necesidades de TODODROGAS CIA S.A.S., cuyo objetivo es proteger y preservar la integridad, confidencialidad y disponibilidad de la información y datos personales.

Asimismo, garantizamos que, en la recolección, almacenamiento, uso y/o tratamiento, destrucción o eliminación de la información suministrada, nos apoyamos en herramientas tecnológicas de seguridad e implementamos prácticas de seguridad que incluyen: transmisión y almacenamiento de información sensible a través de mecanismos seguros, uso de protocolos seguros, aseguramiento de componentes tecnológicos, restricción de acceso a la

información sólo a personal autorizado, respaldo de información, prácticas de desarrollo seguro de software, entre otros.

En caso de ser necesario suministrar información a un tercero por la existencia de un vínculo contractual, suscribimos contrato de transmisión para garantizar la reserva y confidencialidad de la información, así como, el cumplimiento de la presente Política del tratamiento de los datos, de las políticas y manuales de seguridad de la información y los protocolos de atención a los titulares establecidos en TODODROGAS CIA S.A.S. En todo caso, adoptamos compromisos para la protección, cuidado, seguridad y preservación de la confidencialidad, integridad y privacidad de los datos almacenados.

20. GESTIÓN DE DOCUMENTOS

Los documentos que contengan datos personales deben ser fácilmente recuperables, es por ello que se debe dejar documentado el lugar donde reposa cada uno de los documentos tanto físicos como digitales, se deben hacer inspecciones a estas rutas de almacenamiento de forma frecuente, se debe garantizar su conservación dejando definido en que soporte y bajo qué condiciones se llevará a cabo esta conservación, teniendo en cuenta condiciones ambientales, lugares de almacenamiento, riesgos a los cuales están expuestos entre otros, el tiempo de retención de los documentos se determina en función de los requisitos legales si aplica, de lo contrario cada organización lo define de acuerdo a sus necesidades, así mismo debe tener clara la disposición final de los mismos, identificando si se recicla, reutiliza, se conserva, se digitaliza entre otros.

Los documentos que tienen que ver con la protección de datos personales deben ser elaborados por personal o una entidad competente para ello, así mismo la organización debe ser quien revise y apruebe todos los documentos y lo deje registrado en la casilla de aprobación de los documentos.

A fin que sean fácilmente trazables, los documentos deberán estar codificados, serán actualizados y modificados por el personal responsable, esta modificación se efectuará siempre y cuando sea necesario, para la eliminación de un documento se debe tener la justificación para ello descrita en el histórico el cual se encuentra en la parte inferior de todos los documentos.

Los documentos tanto físicos como digitales que contengan datos personales, deben ser protegidos por agentes externos o internos que puedan alterar su contenido.
La distribución de los documentos que contengan datos personales la efectuara el responsable del tratamiento, este dejará documentada la evidencia de dicha distribución, donde entre otros se especifique; el tipo de documento y la identificación de la persona a la cual se le entregó la información.

Se deberá designar un responsable de garantizar la confidencialidad de los datos personales de los titulares, este será quien custodie documentos, garantice su protección tanto física como digital, evite alteraciones de la información, así mismo garantizará que los documentos que salgan de su custodia sean identificados y fácilmente trazables.