POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

1. GENERALIDADES.

1.1. RESPONSABLE DE TRATAMIENTO.

MDV DISTRIBUIDORA S.A.S. sociedad constituida y existente bajo las leyes de la República de Colombia, en adelante **MDV**, actuando como responsable del tratamiento de información personal, se identifica a través de los siguientes datos:

Razón social	MDV DISTRIBUIDORA S.A.S.
NIT	901.924.401 – 4
Domicilio	Calle 100 # 8A - 55, Bogotá D.C., Colombia
Correo electrónico	contacto@mdvdistribuidora.com
Teléfono	(+57) 333-603-4902

1.2. DEFINICIONES.

1.2.1. **Autorización:** consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

1.2.2. **Base de Datos:** conjunto organizado de datos personales que sea objeto de Tratamiento.

1.2.3. **Dato personal:** cualquier información vinculada o que pueda asociarse a una o a varias personas naturales determinadas o determinables.

1.2.4. **Dato personal semiprivado:** son aquellos datos que no tienen una naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular, sino a un grupo de personas o a la sociedad en general. En este caso, para su tratamiento se requiere la autorización expresa del Titular de la información. Por ejemplo: datos de carácter financiero, datos relativos a las relaciones con las entidades de seguridad social (EPS, AFP, ARL, Cajas de Compensación).

1.2.5. **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.

1.2.6. **Dato personal 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 expresa. Por ejemplo: Nivel de escolaridad, libros de los comerciantes, entre otros.

1.2.7. **Dato personal público:** es aquel tipo de dato personal que las normas y la Constitución han determinado expresamente como públicos y, para cuya recolección y tratamiento, no es necesaria la autorización del Titular de la información. Por ejemplo: estado civil de las personas, datos contenidos del RUNT, datos contenidos en sentencias judiciales ejecutoriadas, entre otros.

1.2.8. **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.

1.2.9. **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.

1.2.10. **Titular:** persona natural cuyos datos personales sean objeto de Tratamiento.

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

1.2.12. **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.

1.2.13. **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 por el Encargado por cuenta del responsable.

1.3. OBJETIVO GENERAL.

La presente Política de Tratamiento de Datos Personales tiene como propósito establecer los criterios bajo los cuales se realiza el tratamiento de la información personal que reposa en las bases de datos, archivos físicos y digitales de **MDV**, dando así cumplimiento al artículo 15 y 20 de la Constitución Nacional, la Ley 1581 de 2012, el Capítulo 25 del Decreto 1074 de 2015 y la Sentencia C-748 de 2011 y Decreto 1377 de 2013.

1.4. ALCANCE.

Esta política aplica para toda la información personal registrada en las bases de datos de **MDV**, quien actúa en calidad de responsable del tratamiento de datos personales. Así mismo establece los criterios que **MDV** ha incorporado para el tratamiento de los datos personales, los mecanismos para que los titulares puedan ejercer sus derechos, las finalidades, las medidas de seguridad, y otros aspectos relacionados con la protección de la información personal.

La presente Política de tratamiento de datos personales está dirigida a cualquier titular de la información o aquel que actúe como su representante legal y del cual **MDV** haya requerido información personal para el desarrollo de alguna actividad.

2. SOBRE EL TRATAMIENTO DE DATOS.

2.1. TIPOS DE DATOS PERSONALES TRATADOS.

MDV en el desarrollo de sus actividades requiere realizar el tratamiento de las siguientes categorías de datos:

2.1.1. Datos de características personales.
2.1.2. Datos de circunstancias sociales.
2.1.3. Datos de contacto.

2.1.4. Datos de salud.
2.1.5. Datos identificativos.
2.1.6. Datos laborales.
2.1.7. Datos patrimoniales.
2.1.8. Datos públicos.
2.1.9. Datos financieros.
2.1.10. Datos Tecnológicos y estructurales de redes.
2.1.11. Información geográfica.

2.2. TRATAMIENTO AL CUAL SE SOMETEN LOS DATOS PERSONALES.

Los datos personales que son obtenidos por **MDV** están sometidos a los siguientes tratamientos:

2.2.1. Recolección

MDV recolecta información personal a través de diversos medios en el desarrollo de las diferentes actividades relacionadas con su objeto social, y las obligaciones que tiene como prestador de servicios tecnológicos y de retail, y de la misma manera dentro de sus obligaciones como empleador. La información personal será obtenida de tres formas diferentes: a) directamente del titular, b) de un tercero siempre y cuando este cuente con la autorización y c) de fuentes públicas de información.

Así mismo la recolección de información personal podrá llevarse a cabo a través de medios físicos, digitales o electrónicos, y en cada uno de ellos se incorporará un aviso de privacidad y autorización, dando así cumplimiento a los requisitos establecidos en el art. 2.2.2.25.3.2 y 2.2.2.25.3.3 del decreto 1074 de 2015 y obedeciendo los principios de libertad y finalidad del art. 4 de la Ley 1581 de 2012.

2.2.2. Almacenamiento.

El almacenamiento de la información personal contenida en las bases de datos o sistemas de información se encuentra en los servidores propios dentro del país, y en servidores externos de terceros, los cuales cuentan con medidas de seguridad física, técnicas y administrativas, y cuenta con controles de acceso a la información, garantizando el principio de acceso y circulación restringida.
La información personal que se encuentre sujeta a requerimientos de Ley permanecerá almacenada en nuestras bases de datos de acuerdo con lo que para esto la Ley haya establecido, en aquellos casos donde la Ley no se ha pronunciado la información permanecerá mientras que la finalidad para la cual fue recolectada se encuentre vigente.

2.2.3. Circulación.

Por regla general, **MDV** no comparte los datos personales que recolecta con terceros. No obstante, para el cumplimiento efectivo de sus obligaciones puede entregar los datos a otras entidades, amparados en los artículos 2.2.2.25.5.1 y 2.2.2.25.5.2 del decreto 1074 de 2015 que establece que se encuentra permitido la transmisión de datos personales cuando sea necesario 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 o exista un contrato de transmisión de datos personales, que

en todo caso, la aceptación de la presente política será circunstancia suficiente para entender la autorización en lo referente a compartir los datos personales de acuerdo con la necesidad de las operaciones de **MDV.**

2.2.4. Actualización y Divulgación de Políticas de Protección de Datos.

Para garantizar la transparencia y el derecho de los titulares a conocer cualquier modificación en las políticas de protección de datos, la organización implementará un protocolo para la actualización y divulgación de cambios en sus políticas.

2.2.5. Procedimiento de Notificación a los Titulares.

Cada vez que se realicen modificaciones sustanciales en las políticas de tratamiento de datos personales, **MDV** informará a los titulares mediante los siguientes medios:

2.2.5.1. Página web: Se actualizará la versión más reciente de la política de privacidad en el sitio oficial, especificando la fecha de modificación y los aspectos ajustados.

2.2.5.2. Otros canales de comunicación: En caso de cambios que impacten de manera significativa los derechos de los titulares, se podrá notificar a través de mensajes en plataformas digitales, aplicaciones o comunicados físicos.

Además, se garantizará que los titulares puedan acceder en cualquier momento a la versión vigente de la política de privacidad y podrán manifestar su aceptación o ejercer su derecho de oposición si consideran que los cambios afectan su privacidad.

2.2.6. Supresión

La supresión de la información personal que haya sido recolectada se llevará a cabo cuando: (I) no sea necesaria para el cumplimiento de aspectos legales, contractuales, tributarios, financieros, de auditoria o esté cubierta por disposiciones o requerimientos de Ley, (II) No afecte o implique la perdida de trazabilidad o integridad de las bases de datos o sistemas de información donde reposa la información; (III) Se haya cumplido o eliminado la finalidad para la cual fueron recolectados. (IV) Sea solicitada por el titular de los datos o aquel que demuestre que se encuentra autorizado y no vaya en contra de las definiciones anteriores. No obstante, pueda que alguna información se conserve únicamente con fines estadísticos o de auditoría.

2.2.7. Plazos de Retención por Tipo de Dato.

MDV, retendrá los datos tratados u obtenidos por cualquiera de los canales ya mencionados durante el tiempo en que permanezca la necesidad de su retención y tratamiento de acuerdo con la finalidad autorizada por los titulares.

2.2.8. Eliminación Segura de Datos.

Al finalizar el ciclo de vida de los datos personales, se garantizará su eliminación de manera segura, evitando accesos no autorizados o recuperación indebida. Se adoptarán las siguientes prácticas de manera enunciativa y no taxativa:

2.2.8.1. Datos en formato digital: Eliminación mediante métodos de sobreescritura o cifrado irreversible.

2.2.8.2. Datos en formato físico: Destrucción mediante trituración o incineración controlada.

2.2.8.3. Notificación de eliminación: En casos en los que el titular lo solicite o la normativa lo exija, se confirmará la supresión de los datos mediante un certificado de eliminación.

2.3. Usos o finalidades de la recolección de información.

El uso o finalidad que se da a la información personal recolectada de cada tipo de titular es:

Tipos de Titular	Finalidades de Uso
Temporales (personas naturales o jurídicas)	1. Gestionar las relaciones, derechos y deberes que se tienen con los titulares (incluyendo el cumplimiento de obligaciones legales, la administración de solicitudes y el ejercicio de derechos relacionados con el tratamiento de datos personales actualización rectificación y supresión) 2. Adelantar comunicaciones o contacto vía correo electrónico, SMS, teléfono u otro medio, de acuerdo con las permisiones otorgadas por la ley 2300 de 2023. 3. Realizar actividades de gestión administrativa (procesamiento de pagos, gestión de contratos, administración de bases de datos, interacción con proveedores, entre otras). 4. Realizar la verificación de datos y referencias 5. Cumplir con los requisitos legales para la prevención del lavado de activos y financiación del terrorismo 6. Realizar la verificación de datos o referencias suministradas con terceros o entidades 7. Cumplir con la atención de derechos de los ciudadanos 8. Adelantar investigaciones en caso de presentarse situaciones de riesgo o violaciones a la seguridad 9. Gestionar la seguridad en todos sus aspectos 10. Adelantar campañas de Actualización de datos e información de cambios en el tratamiento de datos personales 11. Realizar la formalización de ajustes o acuerdos de pago 12. Cumplir con los requisitos legales asociados a la formalización de contratos 13. Generar estadísticas internas 14. Cumplir lo dispuesto por el ordenamiento jurídico colombiano en materia de seguridad y salud en el trabajo 15. Cumplir con los requisitos asociados a las relaciones laborales y condiciones de trabajo 16. Adelantar la administración de Sistemas de Información, gestión de claves, administración de usuarios, etc. 17. Trámite de requerimientos por parte de entidades como IPS, EPS, ARL. 18. Gestionar las actividades asociadas al manejo de personal 19. Cumplir lo dispuesto por el ordenamiento jurídico colombiano en materia laboral y de seguridad social.

Tipos de Titular	Finalidades de Uso
	20. Cumplir con los requisitos de gestión de riesgos laborales 21. Preservar la seguridad de los activos y personas 22. Gestionar y realizar el pago de nómina. 23. Adelantar la gestión de riesgos laborales y la prevención y protección del recurso humano ante enfermedades y accidentes del ámbito laboral 24. Registro en aplicativos y formularios de entidades y organismos estatales por requerimiento legal 25. Adelantar procedimientos administrativos y de control interno 26. Realizar procesos de formación de personal interno 27. Realizar y cumplir con las obligaciones legales en materia contable y tributaria.
Proveedores y Contratistas	1. Mantener un registro histórico y estadístico 2. Generar modelos y datos para la toma de decisiones 3. Remitir o enviar información relacionada con el objeto social de la organización, en cumplimiento de la Ley 2300 de 2023. 4. Gestionar las relaciones, derechos y deberes que se tienen con los titulares 5. Realizar el envío de comunicaciones a nivel general (comerciales, informativas, promocionales, transaccionales, relacionadas con cobranzas, etc. De acuerdo con la política de tratamiento de datos, en cumplimiento de la Ley 2300 de 2023) 6. Gestionar y mantener un histórico de relaciones comerciales 7. Realizar la verificación de cumplimientos legales o normativos 8. Realizar actividades de gestión administrativa (procesamiento de pagos, gestión de contratos, administración de bases de datos, interacción con proveedores, entre otras). 9. Realizar la verificación de datos y referencias 10. Recibir y gestionar requerimientos sobre productos o servicios, atención a los titulares (Gestión PQR) 11. Cumplir con los requisitos legales para la prevención del lavado de activos y financiación del terrorismo 12. Realizar la verificación de datos o referencias suministradas con terceros o entidades 13. Cumplir con la atención de derechos de los ciudadanos 14. Adelantar investigaciones en caso de presentarse situaciones de riesgo o violaciones a la seguridad 15. Realizar actividades de cobro y pago 16. Adelantar campañas de Actualización de datos e información de cambios en el tratamiento de datos personales 17. Realizar la formalización de ajustes o acuerdos de pago 18. Cumplir con los requisitos legales asociados a la formalización de contratos 19. Cumplir lo dispuesto por el ordenamiento jurídico colombiano en materia de seguridad y salud en el trabajo 20. Trámite de requerimientos por parte de entidades como IPS, EPS, ARL. 21. Adelantar procedimientos administrativos y de control interno 22. Realizar la verificación de requisitos jurídicos, técnicos y/o financieros

Tipos de Titular	Finalidades de Uso
	23. Gestionar las relaciones, derechos y deberes que se tienen con proveedores
Clientes	1. Mantener un registro histórico y estadístico de las relaciones comerciales 2. Generar modelos y datos para la toma de decisiones 3. Atender requerimientos de autoridades judiciales o administrativas 4. Remitir o enviar información relacionada con el objeto social de la organización 5. Gestionar las relaciones, derechos y deberes que se tienen con los titulares 6. Realizar el envío de comunicaciones a nivel general(comerciales, informativas, promocionales, transaccionales, relacionadas con cobranzas, etc. De acuerdo con la política de tratamiento de datos, en cumplimiento de la Ley 2300 de 2023) 7. Adelantar el ofrecimiento productos y servicios 8. Realizar encuestas de opinión 9. Realizar la verificación de cumplimientos legales o normativos 10. Realizar actividades de gestión administrativa(procesamiento de pagos, gestión de contratos, administración de bases de datos, interacción con proveedores, entre otras). 11. Realizar la verificación de datos y referencias 12. Generar facturas 13. Recibir y gestionar requerimientos sobre productos o servicios, atención a los titulares (Gestión PQR) 14. Cumplir con los requisitos legales para la prevención del lavado de activos y financiación del terrorismo 15. Adelantar comunicaciones a distancia para la venta de productos o servicios 16. Realizar la verificación de datos o referencias suministradas con terceros o entidades 17. Adelantar investigaciones en caso de presentarse situaciones de riesgo o violaciones a la seguridad 18. Enviar y compartir publicidad propia 19. Realizar la aplicación de sanciones asociadas a incumplimientos de algún tipo 20. Cumplir con los deberes económicos y contables de la organización 21. Realizar actividades de cobro y pago 22. Realizar análisis de perfiles 23. Realizar actividades de fidelización 24. Adelantar campañas de Actualización de datos e información de cambios en el tratamiento de datos personales 25. Realizar la formalización de ajustes o acuerdos de pago 26. Realizar actividades de marketing tradicional o digital 27. Cumplir con los requisitos legales asociados a la formalización de contratos
Empleados o exempleados	1. Mantener un registro histórico y estadístico 2. Gestionar las relaciones, derechos y deberes que se tienen con los titulares

Tipos de Titular	Finalidades de Uso
	3. Adelantar comunicaciones o contacto vía correo electrónico, SMS, teléfono u otro medio 4. Realizar actividades de gestión administrativa (procesamiento de pagos, gestión de contratos, administración de bases de datos, interacción con proveedores, entre otras). 5. Realizar la verificación de datos y referencias 6. Cumplir con los requisitos legales para la prevención del lavado de activos y financiación del terrorismo 7. Realizar la verificación de datos o referencias suministradas con terceros o entidades 8. Cumplir con la atención de derechos de los ciudadanos 9. Adelantar investigaciones en caso de presentarse situaciones de riesgo o violaciones a la seguridad 10. Gestionar la seguridad en todos sus aspectos 11. Realizar la aplicación de sanciones asociadas a incumplimientos de algún tipo 12. Adelantar campañas de Actualización de datos e información de cambios en el tratamiento de datos personales 13. Realizar la formalización de ajustes o acuerdos de pago 14. Cumplir con los requisitos legales asociados a la formalización de contratos 15. Cumplir lo dispuesto por el ordenamiento jurídico colombiano en materia de seguridad y salud en el trabajo 16. Cumplir con los requisitos asociados a las relaciones laborales y condiciones de trabajo 17. Adelantar la administración de Sistemas de Información, gestión de claves, administración de usuarios, etc. 18. Trámite de requerimientos por parte de entidades como IPS, EPS, ARL. 19. Gestionar las actividades asociadas al manejo de personal 20. Cumplir lo dispuesto por el ordenamiento jurídico colombiano en materia laboral y de seguridad social, entre otras, aplicables a exempleados o empleados actuales 21. Gestionar y realizar el pago de nómina 22. Realizar la verificación de riesgo de salud 23. Registro en aplicativos y formularios de entidades y organismos estatales por requerimiento legal 24. Cumplir con los requisitos de pago de prestaciones sociales 25. Asegurar la gestión de la seguridad en nuestras instalaciones 26. Adelantar procedimientos administrativos y de control interno 27. Cumplir con la declaración y pago de aportes de seguridad social 28. Realizar procesos de formación de personal interno

2.4. TRATAMIENTO DE DATOS SENSIBLES.

Los datos sensibles recolectados serán tratados con las siguientes finalidades.

Tipo de Dato Sensible	Finalidad de Recolección
Datos de salud	1. Mantener un registro histórico y estadístico 2. Generar modelos y datos para la toma de decisiones 3. Adelantar comunicaciones o contacto vía correo electrónico, SMS, teléfono u otro medio 4. Realizar actividades de gestión administrativa. 5. Generar estadísticas internas 6. Cumplir lo dispuesto por el ordenamiento jurídico colombiano en materia de seguridad y salud en el trabajo 7. Cumplir con los requisitos asociados a las relaciones laborales y condiciones de trabajo 8. Trámite de requerimientos por parte de entidades como IPS, EPS, ARL. 9. Gestionar las actividades asociadas al manejo de personal 10. Cumplir con los requisitos de gestión de riesgos laborales 11. Realizar la verificación de riesgo de salud 12. Adelantar procedimientos administrativos y de control interno 13. Realizar procesos de formación de personal interno 14. Informarle o hacerlo participe de programas de promoción y prevención 15. Gestionar actividades de capacitación

2.5. AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS.

MDV solicitará de manera libre, previa, expresa y debidamente informada, la autorización por parte de los titulares de los datos personales y para ello generará mecanismos idóneos garantizando para cada caso que sea posible verificar el otorgamiento de dicha autorización. La misma podrá constar en cualquier medio, bien sea un documento físico, digital, electrónico o en cualquier formato que garantice su posterior consulta a través de herramientas técnicas, cumpliendo con los requisitos establecidos en la Ley.

2.6. AUTORIZACIÓN TRATAMIENTO DE DATOS NIÑOS, NIÑAS Y ADOLESCENTES.

En el Tratamiento de datos personales de niños, niñas y adolescentes se asegurará el respeto a los derechos de los menores de edad. **MDV** podrá requerir el tratamiento de datos personales de menores de edad para dar cumplimiento a aspectos legales como: I) El artículo 32 de la Ley 789 de 2002 relacionado con la obligación de adelantar la vinculación de aprendices y II) El derecho de los afiliados al Sistema de Seguridad Social de afiliar a cualquier pariente dentro del tercer grado de consanguinidad o a cualquier menor de 12 años (sea o no pariente) siempre y cuando dependa económicamente.

En caso de requerir la recolección directa de datos personales de niños, niñas y adolescentes, **MDV** solicitará la autorización de tratamiento con el consentimiento informado de los padres o adultos responsables de los menores de edad.

2.6.1. Procedimientos específicos para garantizar la protección de los datos de menores de edad.

Para asegurar la confidencialidad, integridad y seguridad de los datos sensibles y de menores, se adoptarán las siguientes medidas:

2.6.1.1. Acceso restringido: Solo el personal autorizado podrá acceder a estos datos, previa validación de su necesidad operativa.
2.6.1.2. Encriptación y almacenamiento seguro: Los datos serán almacenados en sistemas con cifrado de extremo a extremo y protocolos de seguridad que permitan dar cumplimiento a la finalidad de protección de los mismos.
2.6.1.3. Minimización de datos: Solo se recolectará y almacenará la información estrictamente necesaria para cumplir con las finalidades autorizadas.
2.6.1.4. Protocolos de auditoría y control: Se realizarán revisiones periódicas para garantizar que el tratamiento de estos datos cumpla con las normas de seguridad y privacidad establecidas.

2.6.2. Mecanismos de verificación del consentimiento informado otorgado por padres o responsables.

Dado que los datos de menores requieren una protección reforzada, se implementarán los siguientes mecanismos de verificación para garantizar que el consentimiento informado sea válido y verificable:

2.6.2.1. Consentimiento expreso y verificable: Se exigirá la firma de un documento físico o digital con validación de identidad de los padres o representantes legales.
2.6.2.2. Doble autenticación: Se emplearán mecanismos como confirmaciones por correo electrónico o códigos de verificación para asegurar la autenticidad del consentimiento.
2.6.2.3. Registro de consentimiento: Toda autorización otorgada por padres o tutores será archivada y podrá ser consultada en cualquier momento para verificar su legitimidad.
2.6.2.4. Facilidades para revocación: Se garantizará que los responsables legales puedan revocar el consentimiento en cualquier momento mediante procedimientos ágiles y accesibles.

2.6.3. Limitación estricta del tratamiento de datos sensibles.

El tratamiento de datos sensibles estará sujeto a un principio de necesidad y proporcionalidad, asegurando que:

2.6.3.1. Se limita a las finalidades estrictamente esenciales, como cumplimiento de normativas legales o prestación de servicios específicos que requieran dichos datos.
2.6.3.2. No se utilicen para fines adicionales no informados o no autorizados por los titulares.
2.6.3.3. Se realiza una evaluación de impacto en la privacidad (EIP) antes de cualquier nuevo proceso que implique la recolección y uso de datos sensibles.

2.7. TRAZABILIDAD DE LAS AUTORIZACIONES EN EL TRATAMIENTO DE DATOS PERSONALES.

En cumplimiento de los artículos 7 y 8 de la Ley 1581 de 2012, se implementarán mecanismos de trazabilidad que permitan verificar, en cualquier momento, la validez y legalidad de las autorizaciones otorgadas por los titulares o sus representantes legales en el caso de menores de edad.
Para garantizar la adecuada gestión de las autorizaciones, se adoptarán los siguientes procedimientos:

2.7.1. Registro de Autorizaciones.

Todas las autorizaciones otorgadas por los titulares se documentarán de manera verificable, asegurando que sean accesibles para su consulta cuando sea necesario. Se establecerán dos tipos de registros:

2.7.1.1. Registros Electrónicos: Se almacenarán en bases de datos seguras con mecanismos de cifrado, asegurando su integridad y disponibilidad. Cada autorización incluirá datos como la fecha, la finalidad del tratamiento, el medio por el cual fue obtenida y la identidad del otorgante.

2.7.1.2. Registros Físicos: Cuando la autorización se obtenga de manera presencial o en papel, se archivará de forma segura, con acceso restringido y mecanismos de control que garanticen su conservación y autenticidad.

2.7.2. Verificación y Control de Autorizaciones.

Para asegurar la autenticidad y validez de las autorizaciones, se aplicarán las siguientes medidas:

2.7.2.1. Doble validación: En el caso de registros electrónicos, se implementará un sistema de confirmación mediante correo electrónico o códigos de autenticación.

2.7.2.2. Auditorías periódicas: Se realizarán revisiones regulares para verificar que todas las autorizaciones almacenadas cumplan con los requisitos legales y que no hayan sido alteradas.

2.7.2.3. Historial de modificaciones: Se mantendrá un registro de cualquier cambio en las autorizaciones, garantizando que las modificaciones sean verificables y trazables.

2.8. Acceso y Disponibilidad de las Autorizaciones.

Los titulares, o sus representantes en el caso de menores, podrán solicitar en cualquier momento acceso a la autorización otorgada, de acuerdo con los derechos de acceso, actualización y supresión de datos consagrados en la Ley 1581 de 2012.
Asimismo, se establecerán mecanismos para que las autoridades competentes puedan acceder a los registros cuando sea requerido en el marco de auditorías o investigaciones sobre el cumplimiento de la normativa en protección de datos personales.

2.9. Revocación de Autorizaciones.

El sistema de trazabilidad garantizará que, en caso de revocación del consentimiento, la eliminación o restricción del tratamiento de datos personales sea ejecutada de manera efectiva y documentada, dejando constancia de la fecha y motivo de la revocación.

3. MEDIDAS DE SEGURIDAD Y PROTECCIÓN.

MDV ha adoptado las medidas técnicas, jurídicas, humanas y administrativas necesarias para procurar la seguridad de los datos de carácter personal protegiendo la confidencialidad, integridad, uso, acceso no autorizado y/o fraudulento. Así mismo, internamente se han implementado protocolos y lineamientos de seguridad de obligatorio cumplimiento para todo el personal con acceso a datos de carácter personal y a los sistemas de información.

3.1. Obligaciones de los encargados de la información personal.

Las empresas y/o personas externas a **MDV**, que en virtud de una relación contractual realice el tratamiento de datos personales, deberá cumplir con las siguientes obligaciones:

3.1.1. Garantizar al titular el acceso, consulta, actualización, rectificación de sus datos personales.
3.1.2. Solicitar y conservar copia de la respectiva autorización para el tratamiento de datos personales informando la finalidad de la recolección
3.1.3. Conservar la información bajo las condiciones de seguridad que impida la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento
3.1.4. Adoptar un manual interno de políticas que garanticen el cumplimiento de la Ley 1581 de 2012, relativa a la protección de datos personales.
3.1.5. Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
3.1.6. Cumplir con las obligaciones establecidas en el artículo 18 de la Ley 1581 de 2012, y sus respectivos decretos reglamentarios, relativos a la protección de datos personales.

3.2. En caso de operar como encargado de la información.

En los casos de que **MDV** opere como encargado de la información, los Responsables de la información deberán solicitar y conservar la autorización del titular de la información, para el tratamiento de los datos personales por parte nuestra, por lo tanto **MDV** presume que el Responsable de la información, cuenta con las autorizaciones previas y expresas de los titulares con quien tiene contacto, para hacer uso de sus datos personales y suministrará copia de tales autorizaciones en caso de que como encargados lo requiramos, para los fines consagrados en la política de tratamiento de datos personales.

3.3. Subencargados de Tratamiento.

En caso de que **MDV** delegue el tratamiento de datos personales a terceros (subencargados), se implementarán mecanismos para garantizar que dichos subencargados cumplan con los mismos estándares de seguridad, confidencialidad y protección de datos establecidos en la Ley 1581 de 2012.

3.3.1. Selección y Supervisión de Subencargados.

Los subencargados serán seleccionados con base en criterios de idoneidad, experiencia y cumplimiento normativo en materia de protección de datos personales. Se establecerán auditorías y controles periódicos para verificar su cumplimiento con los estándares de seguridad exigidos por la organización.

3.3.2. Obligaciones de Seguridad de los Subencargados.

Todo subencargado deberá implementar medidas de seguridad equivalentes a las exigidas por la organización y responderá por cualquier vulneración de datos personales bajo su responsabilidad. Para ello, deberá garantizar:

3.3.2.1. Implementación de medidas técnicas y organizativas adecuadas para prevenir accesos no autorizados, pérdida o alteración de los datos.
3.3.2.2. Confidencialidad y tratamiento de datos únicamente para las finalidades definidas por la organización.
3.3.2.3. Restricción de acceso a la información solo a personal autorizado.

4. CAPACITACIÓN Y FORMACIÓN DEL PERSONAL EN PROTECCIÓN DE DATOS.

Para garantizar el cumplimiento de los principios de confidencialidad, seguridad y legalidad en el tratamiento de datos personales, la organización establecerá un programa de capacitación continua dirigido a todos los colaboradores que manejan información personal.

4.1. Programa de Capacitación en Protección de Datos Personales.

4.1.1. Objetivo.

Garantizar que los empleados adquieran las herramientas y conocimientos necesarios para un adecuado tratamiento de datos personales, minimizando riesgos y asegurando el cumplimiento normativo.

4.1.2. Contenido de la Capacitación

4.1.2.1. **Principios de Protección de Datos:** Explicación de la Ley 1581 de 2012, incluyendo transparencia, confidencialidad, acceso restringido y seguridad de la información.
4.1.2.2. **Gestión de Datos Sensibles:** Procedimientos para el manejo de información de menores y datos sensibles.
4.1.2.3. **Seguridad de la Información:** Buenas prácticas en ciberseguridad, prevención de filtraciones y accesos no autorizados.
4.1.2.4. **Identificación y Reporte de Incidentes:** Protocolo para detectar, reportar y responder a incidentes de seguridad.
4.1.2.5. **Obligaciones Legales y Éticas:** Responsabilidades del personal, sanciones y consecuencias del incumplimiento.

4.1.3. Metodología y Frecuencia.

4.1.3.1. Capacitaciones periódicas con sesiones iniciales para nuevos empleados y actualizaciones anuales.
4.1.3.2. Métodos interactivos como talleres, simulaciones, e-learning y evaluaciones.
4.1.3.3. Participación obligatoria para quienes manejen datos personales.

4.1.4. Compromiso de la Organización.

Se garantizará formación continua y cumplimiento de procesos internos alineados con la normativa de protección de datos.

5. GESTIÓN DE DERECHOS DE LOS TITULARES.

5.1. Derechos de los Titulares.

Los titulares pueden:

5.1.1. Acceder gratuitamente a sus datos personales.
5.1.2. Conocer, actualizar y rectificar información inexacta o incompleta.
5.1.3. Conocer el propósito del tratamiento de sus datos.
5.1.4. Revocar la autorización y solicitar la supresión de datos (salvo impedimentos legales o contractuales).
5.1.5. Presentar quejas ante la Superintendencia de Industria y Comercio (SIC) si **MDV** no responde satisfactoriamente.
5.1.6. Solicitar prueba de la autorización otorgada para el tratamiento.
5.1.7. Abstenerse de responder preguntas sobre datos sensibles o de menores.

5.2. Tiempos de Atención.

5.2.1. Consultas: Respuesta en máximo 10 días hábiles, prorrogable por 5 días adicionales con justificación.
5.2.2. Reclamos: Respuesta en máximo 15 días hábiles, prorrogable por 8 días adicionales con justificación.
5.2.3. Si el reclamo es incompleto, se requerirá al titular dentro de los 5 días siguientes; si no responde en 2 meses, se entenderá desistido.
5.2.4. Si **MDV** no es competente, remitirá el reclamo en máximo 2 días hábiles e informará al titular.

5.3. Procedimiento para el Ejercicio de Derechos.

5.3.1. Titulares o Representantes Autorizados.

Pueden ejercer sus derechos: temporales, proveedores, contratistas, clientes, empleados o exempleados.

5.3.1.1. Información Requerida.

5.3.1.1.1. Nombre completo, identificación y datos de contacto.
5.3.1.1.2. Motivo del reclamo y derecho que desea ejercer.
5.3.1.1.3. Firma e identificación.
5.3.1.1.4. Documentos que acrediten representación si aplica.

5.3.1.2. Solicitudes de Imágenes o Videos.

5.3.1.2.1. Indicar fecha, hora y lugar del material requerido.
5.3.1.2.2. Justificar la solicitud.
5.3.1.2.3. Aportar documentos que acrediten legitimación.
5.3.1.2.4. **MDV** verificará la existencia del material y si compromete la privacidad de terceros, notificará al solicitante y ofrecerá la opción de anonimización, cuyos costos asumiría el solicitante.

5.3.1.2.5. Si no hay afectación a terceros, el titular podrá visualizar la información en las instalaciones de la empresa.

5.3.1.3. Canales y Responsable.
Los titulares pueden ejercer sus derechos a través de:

5.3.1.3.1. Correo electrónico: contacto@mdvdistribuidora.com
5.3.1.3.2. Teléfono: (+57) 333-603-4902
5.3.1.3.3. Punto de recepción documental: Calle 100 # 8A - 55, Bogotá D.C., Colombia.

El cumplimiento de la política será responsabilidad de la Responsable del Sistema de Gestión Integrado, quien podrá solicitar apoyo a otras áreas.

6. ASPECTOS FINALES.

6.1. Notificación de Incidentes de Seguridad.

Se implementará un procedimiento formal para notificar incidentes de seguridad a los titulares y a la Superintendencia de Industria y Comercio.

6.2. Procedimiento de Notificación.

6.2.1. Identificación y Evaluación del Incidente: Análisis del tipo de datos comprometidos y la causa del incidente.
6.2.2. Medidas de Contención: Implementación inmediata de controles para mitigar daños.
6.2.3. Notificación a la Autoridad y a los Titulares: Informar a la SIC y a los afectados sobre el incidente y las medidas adoptadas.
6.2.4. Acciones Correctivas: Implementación de mejoras para evitar incidentes futuros.

Última actualización: 18 de marzo de 2025.