MANUAL DE PROTECCIÓN DE DATOS PERSONALES

EMISIÓN	19/09/2025
ACTUALIZACIÓN	19/09/2025
VERSIÓN	01
CÓDIGO	MG-MAN-007

TABLA DE CONTENIDO

1. Objetivo

Establecer los lineamientos para el adecuado tratamiento de los datos personales en Mastín Seguridad LTDA, garantizando el cumplimiento de la normativa vigente y el respeto por los derechos de los titulares. Con ello, se busca:

- ✓ Garantizar la protección y privacidad de los datos personales de clientes, empleados, proveedores y demás partes interesadas, asegurando su tratamiento conforme a los principios de legalidad, finalidad, libertad, veracidad, transparencia, seguridad, acceso y circulación restringida.
- ✓ Definir los procedimientos internos para la recopilación, almacenamiento, uso, transferencia y eliminación de datos personales, asegurando que se realicen de manera segura y responsable.
- ✓ Establecer mecanismos de control y seguridad que minimicen riesgos de acceso no autorizado, alteración, pérdida o divulgación indebida de la información personal bajo custodia de la empresa.
- ✓ Brindar claridad sobre los derechos de los titulares, incluyendo el acceso, actualización, rectificación y supresión de sus datos, así como los procedimientos para ejercerlos.
- ✓ Garantizar la transparencia en el tratamiento de los datos, mediante la implementación de canales de comunicación efectivos para atender consultas y reclamos relacionados con la protección de la información personal.
- ✓ Promover una cultura de protección de datos dentro de la empresa, capacitando a los colaboradores sobre la importancia del cumplimiento de esta política y las medidas de seguridad aplicables.
- ✓ Asegurar el cumplimiento normativo, alineando las prácticas empresariales con la legislación vigente en Colombia y adoptando estándares internacionales de protección de datos cuando sea pertinente.

2. Alcance

La Política de Protección de Datos Personales de Mastín Seguridad LTDA se aplica a la recopilación, almacenamiento, uso, circulación y eliminación de datos personales de clientes, empleados y proveedores, garantizando el cumplimiento de la normativa vigente en Colombia. La empresa se compromete a adoptar medidas de seguridad y procedimientos internos que protejan la información, asegurando su tratamiento conforme a los principios de legalidad, finalidad, libertad, veracidad, transparencia y seguridad.

Esta política cubre todos los procesos relacionados con el manejo de datos personales dentro de Mastín Seguridad LTDA, incluyendo la gestión de consultas y reclamos de los titulares. Asimismo, establece mecanismos de control para minimizar riesgos de acceso no autorizado, pérdida o uso indebido de la información. En caso de operaciones internacionales, se

aplicarán estándares adecuados de protección para garantizar la seguridad y confidencialidad de los datos tratados.

Identificación del responsable

Responsable	MASTIN SEGURIDAD LTDA
Ocupación	Empresa especializada en la prestación de servicios integrales de seguridad, ofreciendo vigilancia fija y móvil con y sin armas, escoltas para protección personal y ejecutiva, soluciones tecnológicas como monitoreo remoto, CCTV y control de accesos, así como asesoría, consultoría e investigación en seguridad para diversos sectores.
Teléfono:	6012406791
Dirección:	Calle 67 D Bis. 65 A 04
E-mail:	sarlaft@mastinseguridad.com e info@alzateyasociados.com
Web Site	www.mastinseguridad.com

3. Definiciones y conceptos claves

- Acceso autorizado: Permiso dado a un usuario para usar ciertos recursos, generalmente después de ingresar un usuario y contraseña correctos.
- Autenticación: Proceso para verificar la identidad de un usuario.
- Autorización: Consentimiento previo, expreso e informado del Titular para tratar sus datos personales.
- Aviso de privacidad: Comunicación al Titular sobre las políticas de tratamiento de sus datos personales y las finalidades del tratamiento.
- Base de Datos: Conjunto organizado de datos personales o cualquier tipo de información que puede ser manejado y procesado por sistemas de información.
- Bases de Datos Automatizadas: Bases de datos que utilizan sistemas informáticos para el tratamiento y gestión de la información, permitiendo realizar operaciones como recolección, almacenamiento, procesamiento y consulta de datos de manera automática.
- Bases de Datos No Automatizadas: Bases de datos gestionadas y mantenidas manualmente sin el uso de sistemas informáticos, utilizando métodos físicos como archivos en papel y registros manuales.
- Contraseña: Seña secreta que permite el acceso autorizado a dispositivos o información.

- Control de acceso: Mecanismo que permite acceder a dispositivos o información mediante autenticación.
- Copia de respaldo: Copia de datos que permite su recuperación en caso de pérdida o daño de los originales.
- Dato personal: Información que puede asociarse a una persona, como nombre, identificación, dirección, etc.
- Dato público: Información no privada ni sensible, como el estado civil o la profesión.
- Dato semiprivado: Información que no es de naturaleza íntima, reservada ni pública, cuyo conocimiento o divulgación puede interesar a cierto sector o grupo de personas, como la información financiera y crediticia.
- Datos sensibles: Información que afecta la intimidad del Titular o puede generar discriminación, como origen racial, salud, vida sexual, datos biométricos o creencias religiosas.
- Encargado del tratamiento: Persona o entidad que trata datos personales por cuenta del responsable.
- Identificación: Proceso de reconocimiento de la identidad de los usuarios.
- Incidencia: Anomalía que afecta la seguridad de los datos.
- Perfil de usuario: Grupo de usuarios con acceso a ciertos recursos.
- Recurso protegido: Componentes del sistema de información, como bases de datos o programas, que requieren medidas de seguridad para su protección.
- Responsable de seguridad: Persona designada para controlar y coordinar las medidas de seguridad de la información.
- Sistema de información: Conjunto de bases de datos y equipos para tratar datos personales.
- Responsable del tratamiento: Persona o entidad que decide sobre el tratamiento de los datos personales.
- Soporte: Material donde se registra o guarda información, como papel, discos, etc.
- Usuario: Persona autorizada para acceder a datos o recursos.
- Titular: Persona cuyos datos personales son objeto de tratamiento.
- Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, como recolección, almacenamiento, uso, circulación o supresión.
- Transferencia: Envío de datos personales a un receptor, dentro o fuera del país, con fines específicos y bajo ciertas condiciones.
- Transmisión: Comunicación de datos personales para su tratamiento por un encargado, conforme a las instrucciones del responsable del tratamiento.

4. Principios de la protección de datos.

En el ámbito de la protección de datos personales, se establecerán los siguientes principios fundamentales:

Principio de legalidad: El tratamiento de datos, conforme a la Ley de Habeas Data, es una actividad regulada que debe ajustarse a lo estipulado en dicha ley y en las normas complementarias que la desarrollen.

Principio de finalidad: La actividad de tratamiento debe responder a una finalidad legítima, conforme a la Constitución y la ley, la cual deberá ser comunicada al Titular de los datos.

Principio de libertad: El tratamiento de datos solo podrá llevarse a cabo con el consentimiento previo, expreso e informado del Titular. No se permitirá la obtención o divulgación de datos personales sin la autorización adecuada, a menos que exista un mandato legal o judicial que exima ese consentimiento.

Principio de veracidad o calidad: La información que se somete a tratamiento debe ser veraz, completa, exacta, actualizada, verificable y comprensible. Se prohíbe el tratamiento de datos que sean parciales, incompletos, fragmentados o que generen confusiones.

Principio de transparencia: Durante el tratamiento, se debe garantizar el derecho del Titular a acceder, en cualquier momento y sin restricciones, a información sobre la existencia de datos que le afecten, proporcionada por el responsable o el encargado del tratamiento.

Principio de acceso y circulación restringida: El tratamiento de datos se encontrará sujeto a límites derivados de la naturaleza de la información personal, así como de las disposiciones legales y constitucionales correspondientes. Esto implica que solo las personas autorizadas por el Titular y/o aquellas designadas por la ley podrán llevar a cabo dicho tratamiento. Exceptuando la información pública, los datos personales no estarán disponibles en Internet u otros medios de comunicación masiva, a menos que el acceso esté controlado técnicamente, garantizando que solo los Titulares o terceros autorizados por la ley tengan esa información.

Principio de seguridad: La información sujeta a tratamiento por parte del responsable o del encargado, según lo establecido en la Ley de Habeas Data, deberá ser administrada con las medidas técnicas, humanas y administrativas necesarias para asegurar la protección de los registros, evitando su alteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Principio de confidencialidad: Todas las personas que participen en el tratamiento de datos personales no públicos están obligadas a mantener la reserva de la información, incluso después de haber finalizado su relación con las actividades vinculadas al tratamiento. La comunicación o suministro de datos personales solo podrá realizarse en el marco de las actividades autorizadas por la ley y de acuerdo con los términos de esta política.

5. Derechos de los titulares de datos personales

Mastín Seguridad Ltda. garantiza a los titulares de datos personales el ejercicio pleno de sus derechos conforme a la normativa vigente. De acuerdo con la **Ley 1581 de 2012**, los titulares podrán ejercer los siguientes derechos:

Conocer, actualizar y rectificar sus datos personales ante el responsable o encargado del tratamiento, especialmente en casos donde la información sea parcial, inexacta, incompleta, fraccionada, genere confusión o su tratamiento esté prohibido o no autorizado.

Solicitar prueba de la autorización otorgada al responsable del tratamiento, salvo en los casos en que la normativa exima este requisito, conforme a lo establecido en el artículo 10 de la ley.

Recibir información sobre el uso de sus datos personales, previa solicitud, por parte del responsable o encargado del tratamiento.

Presentar quejas ante la Superintendencia de Industria y Comercio por el incumplimiento de disposiciones legales o normativas relacionadas con la protección de datos personales.

Revocar la autorización y solicitar la eliminación de sus datos personales cuando el tratamiento no respete los principios, derechos y garantías constitucionales y legales. Esta solicitud procederá si la Superintendencia de Industria y Comercio determina que el responsable o encargado ha incurrido en conductas contrarias a la ley y la Constitución.

Acceder de manera gratuita a sus datos personales que hayan sido objeto de tratamiento, garantizando transparencia y control sobre su información.

6. Roles y responsabilidades

En *Mastín Seguridad Ltda.*, la gestión de datos personales se basa en una asignación clara de responsabilidades que involucra tanto actores internos como externos, asegurando el cumplimiento del marco legal y la salvaguarda de la información.

6.1. Comité de protección de datos personales

El **Comité de protección de datos** es el órgano responsable de supervisar, analizar y optimizar las políticas y procedimientos de protección de datos. Este comité estará conformado por un delegado del **Gerente General**, el **Oficial de Protección de Datos (DPO)** y líderes de áreas estratégicas. Su misión es garantizar el cumplimiento normativo, identificar riesgos y proponer estrategias de mejora continua. Sesionará ordinariamente cada dos meses y de manera extraordinaria en caso de emergencias o cambios regulatorios significativos.

6.2. Alta Dirección

La **Gerencia General** y demás directivos juegan un papel clave en la protección de datos, asegurando los recursos técnicos, humanos y financieros para la implementación de políticas de seguridad. También lideran la adopción de las políticas internas y supervisan el cumplimiento de los objetivos establecidos por el Comité de protección de datos**.**

6.3. Oficial de Protección de Datos (DPO)

El Oficial de Protección de Datos es el encargado de coordinar la estrategia de cumplimiento en *Mastín Seguridad Ltda*. Supervisa el correcto funcionamiento de los procesos, actúa como

enlace con las autoridades regulatorias, lidera auditorías internas y capacita al personal en buenas prácticas de manejo de información.

6.4. Trabajadores

Cada colaborador de la empresa tiene la obligación de cumplir con las políticas establecidas para la protección de datos. Deben participar en capacitaciones obligatorias, reportar cualquier incidente de seguridad y manejar la información con integridad, transparencia y confidencialidad.

6.5. Aliados y Contratistas

Los aliados estratégicos y contratistas que administran información personal en nombre de *Mastín Seguridad Ltda*. deben adoptar medidas de protección administrativas y técnicas, firmar acuerdos de confidencialidad y reportar cualquier incidente que afecte la integridad de los datos.

6.6. Responsable del Tratamiento

Mastín Seguridad Ltda. es el responsable del tratamiento de datos personales, lo que implica diseñar e implementar políticas para la recolección, almacenamiento, uso, transferencia y supresión de información. También debe atender consultas y reclamos de los titulares y demostrar cumplimiento ante la Superintendencia de Industria y Comercio.

Deberes del Responsable del Tratamiento:

- ✓ Garantizar al titular el ejercicio pleno de su derecho de habeas data.
- ✓ Solicitar y conservar copia de la autorización otorgada por el titular.
- ✓ Informar al titular sobre el propósito de la recolección de datos y sus derechos.
- ✓ Mantener la información en condiciones de seguridad que eviten adulteraciones o accesos no autorizados.
- ✓ Asegurar que los datos entregados al encargado del tratamiento sean veraces, completos y actualizados.
- ✓ Actualizar y rectificar la información cuando sea necesario.
- ✓ Exigir al encargado del tratamiento el respeto por la seguridad y privacidad de la información.
- ✓ Tramitar consultas y reclamos conforme a la Ley 1581 de 2012.
- ✓ Adoptar un manual interno de políticas y procedimientos para garantizar el cumplimiento legal.
- ✓ Notificar a la autoridad de protección de datos en caso de incidentes que comprometan la seguridad de la información.
- ✓ Cumplir con los requerimientos de la Superintendencia de Industria y Comercio.

6.7. Encargado del Tratamiento

El encargado del tratamiento (ya sea un área interna o un tercero contratado) debe aplicar medidas de seguridad para prevenir accesos no autorizados, fugas de información o pérdida de datos. Además, tiene la obligación de informar al responsable sobre cualquier irregularidad detectada.

7. Autorización del Tratamiento de Datos Personales

Mastín Seguridad Ltda. garantiza que el tratamiento de datos personales se realizará con autorización previa e informada del titular, en cumplimiento de la **Ley Estatutaria 1581 de 2012** y sus reglamentaciones. Dicha autorización podrá ser obtenida a través de cualquier medio que permita su consulta posterior, asegurando transparencia y control sobre la información. Sin embargo, no será necesario contar con el consentimiento del titular en los siguientes casos:

- Cuando la información sea solicitada por una entidad pública o administrativa en el ejercicio de sus funciones legales o por orden judicial.
- Para datos de naturaleza pública según lo dispuesto en la normativa vigente.
- En situaciones de urgencia médica o sanitaria, donde el acceso a la información sea crucial para preservar la vida o integridad del titular.
- Cuando el tratamiento esté autorizado por la ley con fines históricos, estadísticos o científicos, garantizando el uso responsable de los datos.
- En relación con los datos registrados en el Registro Civil de las Personas, conforme a la normatividad establecida.

8. Tipo de Información Recolectada

Mastín Seguridad Ltda. recopila información personal de clientes, empleados, contratistas, proveedores y otras personas vinculadas a sus operaciones, con el propósito de garantizar la seguridad y optimizar la prestación de sus servicios. Los datos recolectados incluyen nombres, apellidos, identificación, información de contacto (correos electrónicos, números telefónicos y direcciones físicas), así como datos relacionados con antecedentes laborales, referencias comerciales y requerimientos específicos de seguridad.

Dependiendo del tipo de servicio prestado, también se podrá recolectar información sobre condiciones de movilidad, ubicación geográfica en tiempo real para operativos de escolta y seguridad privada, registros de acceso a instalaciones protegidas, videovigilancia en tiempo real y documentación requerida para la gestión de permisos y certificaciones.

El tratamiento de estos datos tiene como finalidad asegurar la correcta ejecución de los servicios de seguridad física, vigilancia fija y móvil con armas y sin armas, escoltas, asesorías y consultoría en seguridad, así como la implementación de soluciones tecnológicas para el monitoreo y control de riesgos. Además, *Mastín Seguridad Ltda*. utiliza esta información para

gestionar protocolos de prevención, garantizar la protección de personas y bienes, y cumplir con las disposiciones normativas aplicables en el sector de seguridad privada.

Todos los datos recopilados son tratados con estricta confidencialidad, en cumplimiento de la normativa vigente, asegurando su uso exclusivo para los fines autorizados por los titulares y dentro del marco de seguridad establecido por la empresa.

8.1. Datos de Niños, Niñas y Adolescentes

Mastín Seguridad Ltda. gestiona el tratamiento de datos personales de niños, niñas y adolescentes en dos ámbitos principales: laboral y bienestar laboral, asegurando su protección conforme a la normativa vigente y bajo principios de confidencialidad, seguridad y transparencia.

Ámbito Laboral. En el contexto laboral, la empresa puede recopilar y tratar información de menores de edad que sean hijos de los trabajadores, con el objetivo de gestionar su afiliación a sistemas de seguridad social, incluyendo EPS, cajas de compensación y seguros. Estos datos son necesarios para garantizar el acceso a beneficios legales y protección en salud, así como para cumplir con obligaciones laborales en el marco de bienestar social.

Bienestar Laboral. En el ámbito del bienestar laboral, la empresa recopila y trata datos personales de menores como parte de programas de bienestar dirigidos a los hijos de sus empleados. Esto incluye actividades recreativas, capacitaciones, apoyos educativos y beneficios adicionales promovidos por la organización. La recopilación de esta información se realiza con el consentimiento expreso de los padres o tutores legales, asegurando el adecuado acceso a los programas de bienestar.

Adicionalmente, en la prestación de servicios de vigilancia en colegios, propiedades horizontales y otros espacios donde haya presencia de menores, Mastín Seguridad Ltda. puede recopilar información esencial para la seguridad, tales como registros de ingreso y salida, monitoreo mediante circuitos cerrados de televisión (CCTV) y documentación de incidentes, con el fin de prevenir riesgos y garantizar la protección de los menores en entornos supervisados.

En casos donde se requiera documentar actividades mediante imágenes o videos, Mastín Seguridad Ltda. garantizará el respeto a la privacidad de los menores, asegurando que cualquier material visual se utilice exclusivamente con fines institucionales y previa autorización de los responsables legales.

9. Finalidades del tratamiento de datos

TIPO DE BASE DE DATOS	FINALIDAD
Empleados	Los datos serán utilizados con las siguientes finalidades: Solicitud de datos concernientes a identificación personal; información de contacto; Datos de carácter académico; Datos del historial laboral, profesional y financiero; Desarrollar adecuadamente el proceso de registro y vinculación laboral; Implementar acciones de bienestar laboral; difundir ofertas laborales para participar en procesos internos de selección; Comunicar información institucional; Ejecutar actividades con fines estadísticos; Desarrollar adecuadamente el proceso de actualización de los datos; Desarrollar los procesos de inscripción en congresos; Eventos o seminarios organizados; Adelantar la actualización de datos y verificación de identidad de los trabajadores y sus familiares (pareja, padres hijos); Citar a los aspirantes en proceso de selección a las entrevistas programadas; Realización de visitas domiciliarias, Realizar estudio de confiabilidad, Realizar estudio de seguridad; Verificación de referencias laborales, personales, experiencia laboral y trayectoria profesional; Suministro de información a las empresas con la cuales se tiene convenio, Confección de artículos de dotación, Envío de información a través de mensajes de texto y correos electrónicos, Entrega y asignación de equipos a los colaboradores; Redacción de informes de gestión humana; Proceso de afiliación al sistema de seguridad social y cajas de compensación del colaborador y sus beneficiarios; Entrega de referencias laborales, Uso de imágenes fotográficas y videos con fines corporativos, Obtención y suministro de datos de los hijos de los colaboradores en el desarrollo de actividades recreativas y de bienestar a través de la Instituciones o entidades aliadas, Evaluaciones de desempeño; Generación de certificaciones laborales, de ascenso, traslado, entrevista de retiro, en procesos de auditoría y control interno y externo, en la entrega de reportes obligatorios institucionales en entrevistas de retiro, Desactivación de sistemas de información; Uso de huellas

TIPO DE BASE DE DATOS	FINALIDAD
	digitales y demás datos de salud y/o datos sensibles para los fines misionales; las anteriores finalidades son enunciativas y no taxativas.
Clientes	Los datos serán utilizados con las siguientes finalidades: Contiene la información de los clientes; Validaciones y análisis relacionadas con el Sistema de Administración de Riesgo de Lavado de Activos y en contra de la Financiación del Terrorismo SARLAFT, la prevención contra el soborno transnacional y las demás que la normatividad colombiana disponga; en la transmisión de los datos a las entidades que regulan el negocio en temas tributarios y aduaneros; gestionar trámites como solicitudes, quejas y/o reclamos, reportes a centrales de riesgo por incumplimiento de las obligaciones financieras derivadas de la relación comercial, envío de comunicaciones a través de mensajes de texto y correos electrónico; para llevar un historial de consumo, Uso de imágenes fotográficas y videos con fines corporativos, Gestión comercial, Conocer información del comportamiento de los clientes de las tiendas, de los clientes institucionales y de E-commerce y sus canales de contacto para realizar ofrecimientos ajustados a sus necesidades; envío de información de los productos, servicios o novedades de la compañía, Conservar registros históricos y mantener contacto comercial; Se realizará el envío de la información otorgada y autorizada por el titular las entidades con las cuales se tienen convenios, estas transferencias estarán siempre mediadas por un documento que garantice que el tratamiento que se le dará a sus datos será el mandado por la normatividad vigente. Las anteriores finalidades son enunciativas y no taxativas.
Proveedores	Los datos serán utilizados con las siguientes finalidades: Solicitud de ofertas y propuestas económicas para la adquisición de productos y servicios; para el análisis y viabilidad de cada producto y/o servicio; envío de comunicaciones a través de mensajes de texto y correos electrónico; presentación de informes pertinentes a los

TIPO DE BASE DE DATOS	FINALIDAD
	diferentes entes de control; revisión y verificación de referencias comerciales; gestiones pre contractuales y contractuales; suministro de información en procesos de auditoría interna y externa que se realicen al interior de la institución; envío de información de los productos, servicios o novedades de la fundación; rastreo en bases de datos restrictivas tales como (policía, procuraduría, contraloría, SARLAFT – Sistema de Administración de Riesgo de Lavado de Activos y Financiación del Terrorismo y las demás que la normatividad colombiana disponga) las anteriores finalidades son enunciativas y no taxativas.
VideoVigilancia	Los datos serán utilizados con las siguientes finalidades: monitoreo y control para la vigilancia de entrada, salida y tráfico de personas dentro de la compañía; control de ingreso y salida de vehículos de los parqueaderos; monitoreo de incidentes para registrar actividades y capturar evidencia visual y auditiva; medida de disuasión de conductas irregulares de terceros mediante la presencia visible de sistemas de video vigilancia; monitoreo y control de la prestación de los servicios institucionales para supervisar y evaluar la correcta ejecución de los mismos; envío de la información otorgada y autorizada por el titular a las entidades con las cuales se tienen convenios, asegurando que estas transferencias estén mediadas por un documento que garantice que el tratamiento de sus datos será conforme a la normativa vigente.
Socios	Los datos serán utilizados con las siguientes finalidades: Contiene la información de los socios; Validaciones y análisis relacionadas con el Sistema de Administración de Riesgo de Lavado de Activos y en contra de la Financiación del Terrorismo SARLAFT, la prevención contra el soborno transnacional y las demás que la normatividad colombiana disponga; en la transmisión de los datos a las entidades que regulan el negocio en temas tributarios y aduaneros; gestionar trámites como solicitudes, quejas y/o reclamos, reportes a centrales de riesgo por

TIPO DE BASE DE DATOS	FINALIDAD
	incumplimiento de las obligaciones financieras derivadas de la relación comercial, envío de comunicaciones a través de mensajes de texto y correos electrónico; para llevar un historial de consumo, Uso de imágenes fotográficas y videos con fines corporativos, Gestión comercial, Conocer información del comportamiento de los socios; envío de información de los productos, servicios o novedades de la compañía, Conservar registros históricos de la compañía y mantener contacto comercial; Se realizará el envío de la información otorgada y autorizada por el titular las entidades con las cuales se tienen convenios, estas transferencias estarán siempre mediadas por un documento que garantice que el tratamiento que se le dará a sus datos será el mandado por la normatividad vigente. Las anteriores finalidades son enunciativas y no taxativas
Seguridad y salud en el trabajo	Los datos serán utilizados con las siguientes finalidades: para la gestión de la seguridad y salud en el trabajo, incluyendo la remisión de los trabajadores a exámenes médicos de ingreso, periódicos y de retiro, y la implementación de programas de vigilancia epidemiológica basados en los conceptos derivados de estos exámenes; en la investigación epidemiológica relacionada con la salud en el trabajo; para brindar información sobre las campañas de salud ocupacional y prevención de riesgos laborales; en la creación de material audiovisual corporativo que promueva la salud y seguridad en el trabajo; para gestionar la comunicación interna sobre el estado de salud general de los trabajadores sin revelar detalles clínicos específicos; llevar a cabo actividades de educación al trabajador y su familia sobre salud y seguridad en el trabajo; enviar información a las Entidades Administradoras de Riesgos Laborales (ARL) y otras entidades con las cuales se tienen convenios, asegurando que el tratamiento de los datos sea conforme a la normatividad vigente; realizar auditorías internas y externas de los sistemas de gestión de seguridad y salud en el trabajo; seguir el estado de salud

TIPO DE BASE DE DATOS	FINALIDAD
	de los trabajadores después de incidentes laborales; enviar información mediante mensajes de texto y correos electrónicos sobre actividades y programas de salud ocupacional, así como confirmaciones de citas médicas relacionadas con la salud en el trabajo; realizar encuestas de satisfacción de los servicios de salud ocupacional recibidos; gestionar las comunicaciones radicadas por los trabajadores (felicitaciones, quejas, peticiones y sugerencias) y su seguimiento; las anteriores finalidades son enunciativas y no taxativas.
Cartera	Los datos serán utilizados con las siguientes finalidades: Reporte Data Crédito; previa solicitud de autorización de acuerdo con la ley 1266 de 2008 Habeas data financiero; envío de información con motivos promocionales y/o informativos mediante mensajes de texto y correos electrónicos las anteriores finalidades son enunciativas y no taxativas.
Aspirantes	Los datos serán utilizados con las siguientes finalidades: para gestionar el proceso de selección y contratación, incluyendo la evaluación y verificación de las competencias y experiencia de los aspirantes; contactarlos para coordinar entrevistas, pruebas y otras etapas del proceso de selección; mantener una base de datos de candidatos para futuras oportunidades laborales; enviar información en mensajes de texto y correos electrónicos con motivos informativos relacionados con el proceso de selección; uso de imágenes fotográficas y videos con fines corporativos durante el proceso de selección, como parte de la documentación de las entrevistas o eventos corporativos; las anteriores finalidades son enunciativas y no taxativas.
Aprendices	Los datos serán utilizados con las siguientes finalidades: para hacer seguimiento y evaluar el desempeño de los practicantes en sus diferentes frentes de trabajo dentro de la empresa; realizar acciones de mejora y apoyo en función de su desempeño; uso de imágenes fotográficas y

TIPO DE BASE DE DATOS	FINALIDAD
	videos con fines corporativos y académicos; las anteriores finalidades son enunciativas y no taxativas.
Convenios	Los datos serán utilizados con las siguientes finalidades: para la entrega de información de los trabajadores y clientes, siempre bajo el acuerdo y para el objeto específico de cada convenio; para el envío de información con motivos promocionales y/o informativos mediante mensajes de texto y correos electrónicos; para la entrega de datos a organismos de control, certificadores o acreditadores de calidad con el fin de soportar requerimientos administrativos, técnicos y científicos; las anteriores finalidades son enunciativas y no taxativas.
Archivos inactivos	Los datos serán utilizados con las siguientes finalidades: almacenamiento de la información propiedad de la empresa; con el fin de poder soportar y documentar los diferentes requerimientos administrativos, envío de información con motivos promocionales y/o informativos mediante mensajes de texto y correos electrónicos; las anteriores finalidades son enunciativas y no taxativas.
Visitantes	Los datos serán utilizados con las siguientes finalidades. Identificar los datos personales del visitante que ingresa a las instalaciones de la empresa, Autorizar la entrada a las diferentes áreas o dependencias, envío de información en mensajes de texto y correos electrónico con motivos promocionales y/o informativos; Se realizará el envío de la información otorgada y autorizada por el titular las entidades con las cuales se tienen convenios, estas transferencias estarán siempre mediadas por un documento que garantice que el tratamiento que se le dará a sus datos será el mandado por la normatividad vigente. las anteriores finalidades son enunciativas y no taxativas.

10. Procedimiento para Ejercer Derechos Relacionados con la Protección de Datos Personales

El titular, sus causahabientes, representante y/o apoderado, o cualquier persona designada por acuerdo de las partes, podrá ejercer sus derechos respecto al tratamiento de sus datos personales comunicándose con *Mastín Seguridad Ltda*. mediante solicitud escrita enviada a los correos info@alzateyasociados.com o sarlaft@mastinseguridad.com.

10.1. Consultas.

Los titulares podrán acceder a la información personal registrada en las bases de datos de la empresa y conocer el uso que se le ha dado a sus datos. Una vez recibida la consulta, esta será atendida en un plazo máximo de diez (10) días hábiles, contados a partir de la fecha de recepción.

Si por alguna razón no es posible responder dentro de dicho término, se informará al solicitante sobre los motivos de la demora y se establecerá una nueva fecha de respuesta, la cual no podrá exceder los cinco (5) días hábiles adicionales.

10.2. Reclamos.

Si el titular considera que su información debe ser corregida, actualizada o eliminada, o si detecta un posible incumplimiento de los deberes establecidos en la normativa de protección de datos personales, podrá presentar un reclamo conforme a los siguientes pasos: El reclamo deberá enviarse por escrito a info@alzateyasociados.com o sarlaft@mastinseguridad.com, incluyendo:

- Identificación del titular (nombre y número de documento).
- Descripción detallada de los hechos que motivan el reclamo.
- Dirección de contacto, tanto física como electrónica (e-mail).
- Documentación de respaldo que sustente la solicitud.

Si el reclamo se presenta incompleto,

*Mastín Seguridad Ltda.*notificará al solicitante dentro de los cinco (5) días siguientes, con el fin de que subsane las deficiencias. Si, tras dos (2) meses, el interesado no proporciona la información adicional, se entenderá que ha desistido del reclamo.

En caso de recibir un reclamo sobre el cual no tenga competencia, *Mastín Seguridad Ltda*. lo remitirá al área correspondiente en un plazo máximo de dos (2) días hábiles, informando al titular sobre la transferencia de su solicitud.

Una vez recibido un reclamo completo, se incluirá en la base de datos una anotación con la leyenda “reclamo en trámite”, acompañada de la razón del reclamo, en un plazo no mayor a dos (2) días hábiles. Esta anotación permanecerá hasta que se resuelva la solicitud.

El plazo máximo para resolver el reclamo será de quince (15) días hábiles contados desde el día siguiente a su recepción. Si se requiere una extensión, se informará al titular sobre las

razones y la nueva fecha de resolución, la cual no podrá superar ocho (8) días hábiles adicionales.

11. Contenido Mínimo de la Solicitud.

Las solicitudes de consulta o reclamo respecto al manejo de datos personales deberán cumplir con los siguientes requisitos:

- Dirigida a **Mastín Seguridad Ltda.** Identificación del titular (nombre y número de documento).
- Descripción detallada de los hechos que originan la solicitud.
- Especificación del **objeto de la petición** (consulta, corrección, actualización, eliminación de datos).
- Indicación de la dirección de notificación del titular, tanto física como electrónica.
- Documentación que respalde la solicitud, especialmente en el caso de reclamos.

Si la consulta o reclamo se presenta **de manera presencial**, el titular deberá realizar su solicitud por escrito, cumpliendo los requisitos mencionados sin necesidad de otras formalidades.

11.1. Requisito de Procedibilidad.

El titular, sus causahabientes, representante y/o apoderado, o cualquier persona designada legalmente, podrá presentar una queja ante la Superintendencia de Industria y Comercio únicamente después de haber agotado el procedimiento de consulta o reclamo directamente con *Mastín Seguridad Ltda*.

12. Petición de Actualización y/o Rectificación**.**

Mastín Seguridad Ltda. procederá a actualizar y rectificar, a solicitud del titular, cualquier información personal que sea inexacta, incompleta o desactualizada, siguiendo el procedimiento y los plazos previamente establecidos en esta política. Para ello, el titular deberá enviar su solicitud a través de los canales oficiales de comunicación de la empresa (**info@alzateyasociados.com** o **sarlaft@mastinseguridad.com**), especificando la actualización o rectificación requerida y anexando la documentación que respalde su petición.

13. Revocación de la Autorización y/o Supresión de Datos Personales.

El titular tiene el derecho de revocar en cualquier momento el consentimiento otorgado para el tratamiento de sus datos personales, siempre que no existan restricciones legales o contractuales que lo impidan. Asimismo, podrá solicitar la supresión o eliminación de sus datos personales en los siguientes casos:

- Cuando considere que sus datos han sido tratados en contravención de los principios, deberes y obligaciones establecidos en la normativa vigente.
- Cuando los datos hayan dejado de ser necesarios o pertinentes para el propósito para el cual fueron recolectados.
- Cuando se haya cumplido el plazo necesario para los fines por los cuales fueron obtenidos.

La supresión de datos podrá realizarse **de manera total o parcial**, según lo solicitado por el titular y conforme a los registros, bases de datos o sistemas de almacenamiento utilizados por *Mastín Seguridad Ltda*..

Sin embargo, es importante aclarar que el derecho a la cancelación no es absoluto. En los siguientes escenarios, *Mastín Seguridad Ltda*. podrá **negar la revocación o eliminación** de los datos personales:

- Si el titular tiene un deber legal o contractual que obliga a la empresa a conservar la información.
- Si la eliminación de los datos puede afectar procesos judiciales o administrativos relacionados con investigaciones fiscales, persecución de delitos, obligaciones sancionatorias o responsabilidades regulatorias.
- Si la información es necesaria para proteger derechos legalmente reconocidos, garantizar el interés público o cumplir con disposiciones adquiridas por el titular.

14. Cesión, Transferencia y Transmisión de Datos Personales

Mastín Seguridad Ltda. garantiza que la cesión, transferencia y transmisión de datos personales se realizará en cumplimiento de la normativa aplicable y bajo estrictos principios de seguridad, legalidad y transparencia, asegurando que la información de los titulares sea protegida de acuerdo con los estándares exigidos por la Superintendencia de Industria y Comercio.

Transferencia de Datos a Terceros Países

De acuerdo con el Título VIII de la Ley Estatutaria de Protección de Datos (LEPD), está prohibida la transferencia de datos personales a países que no garanticen niveles adecuados de protección. Se considera que un país ofrece un nivel adecuado cuando cumple con los estándares establecidos por la Superintendencia de Industria y Comercio, conforme a la Circular 005 del 10 de agosto de 2017, asegurando que estos estándares no sean inferiores a los exigidos en Colombia.

Excepciones a la Prohibición de Transferencia

Esta prohibición no se aplicará en los siguientes casos:

- ✓ Cuando el titular haya otorgado su consentimiento expreso e inequívoco para la transferencia de sus datos.
- ✓ En el intercambio de información médica, necesario para el tratamiento del titular por razones de salud o higiene pública.
- ✓ En transacciones bancarias o bursátiles, conforme a la legislación vigente.
- ✓ En transferencias establecidas dentro de tratados internacionales suscritos por Colombia, bajo el principio de reciprocidad.
- ✓ Para la ejecución de un contrato entre el titular y el responsable del tratamiento, o para la adopción de medidas precontractuales, siempre que exista autorización del titular.
- ✓ Cuando sea legalmente necesario para proteger el interés público o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

Declaración de Conformidad

En los casos que no estén cubiertos por las excepciones anteriores, la Superintendencia de Industria y Comercio será la entidad responsable de emitir la declaración de conformidad respecto a la transferencia internacional de datos personales. Para ello, podrá solicitar información y realizar verificaciones necesarias para garantizar el cumplimiento de los requisitos exigidos.

Transmisiones Internacionales de Datos Personales

Las transmisiones internacionales de datos personales, realizadas entre un responsable y un encargado del tratamiento, con el propósito de que el encargado gestione los datos en nombre del responsable, no requieren autorización expresa del titular, siempre que exista un contrato de transmisión de datos personales que cumpla con los siguientes requisitos:

- ✓ Finalidad del Tratamiento: Definir de manera clara el propósito del tratamiento por parte del encargado.
- ✓ Obligaciones del Encargado: Especificar las responsabilidades en cuanto a la protección y confidencialidad de los datos.
- ✓ Derechos del Titular: Garantizar que el tratamiento de datos personales no vulnerará los derechos del titular.
- ✓ Medidas de Seguridad: Establecer controles adecuados para la protección de los datos durante su tratamiento.
- ✓ Términos y Condiciones: Definir la duración del tratamiento, los criterios de cancelación y las obligaciones contractuales.

Obligaciones Adicionales para la Transferencia Internacional de Datos

Mastín Seguridad Ltda. deberá cumplir con las siguientes obligaciones antes de efectuar una transferencia internacional de datos personales:

Evaluación del Nivel de Protección: Se debe realizar una evaluación previa del nivel de protección de datos en el país receptor, garantizando su cumplimiento con los estándares fijados por la Superintendencia de Industria y Comercio.

Notificación a la Superintendencia: En casos de transferencia internacional, se deberá informar a la Superintendencia de Industria y Comercio, proporcionando detalles sobre las medidas implementadas para salvaguardar la información.

Documentación y Registro: Mantener un registro exhaustivo y documentación detallada de todas las transferencias internacionales de datos, incluyendo contratos, evaluaciones de protección y notificaciones enviadas.

15. Uso de Cookies y Datos de Navegación

Cookies. *Mastín Seguridad Ltda*. utiliza cookies en su sitio web con el propósito de analizar el tráfico, mejorar la calidad de navegación y optimizar la experiencia del usuario. La información recolectada será utilizada exclusivamente para fines estadísticos y operativos, asegurando que, una vez cumplidos los objetivos establecidos en esta política, los datos sean eliminados del sistema.

Enlaces a Otros Sitios Web y Correo Electrónico. El sitio web de *Mastín Seguridad Ltda*. puede contener enlaces a páginas externas. Sin embargo, una vez que el usuario abandona el sitio principal, la empresa no tiene control sobre el tratamiento de datos en dichos portales. Por lo tanto, no se asume responsabilidad por la protección y privacidad de la información proporcionada en plataformas de terceros, quedando su manejo sujeto a las políticas de privacidad propias de cada sitio.

Aceptación de la Política de Tratamiento de Datos Personales. La aceptación expresa de esta Política de Tratamiento de Datos Personales se considera válida cuando el usuario proporciona su información mediante cualquier canal de comunicación de la empresa, incluyendo el sitio web, de forma autónoma y libre, ya sea oralmente, por escrito o a través de acciones inequívocas. Para los fines de esta política, se entiende por "tratamiento" cualquier operación realizada sobre datos personales, incluyendo recolección, almacenamiento, uso, transmisión y/o transferencia de información. Con la aceptación de esta política, el titular de los datos autoriza expresamente a *Mastín Seguridad Ltda*. para procesar la información con el objetivo de cumplir con las finalidades descritas en esta política.

Respecto a modificaciones en la política de privacidad y tratamiento de datos, *Mastín Seguridad Ltda*.se reserva el derecho de realizar ajustes o actualizaciones en cualquier momento, ya sea por cambios normativos, actualizaciones internas o nuevas necesidades operativas.

Las modificaciones serán accesibles a través de medios digitales y físicos de la empresa, asegurando que los usuarios puedan consultar la versión actualizada de la política.

16. Gestión de los Riesgos en la Protección de Datos Personales

La gestión de riesgos en *Mastín Seguridad Ltda*. es un pilar fundamental para garantizar la seguridad, confidencialidad y legalidad en el tratamiento de datos personales. Esta sección establece los procedimientos para identificar, analizar y mitigar riesgos asociados con la información, en conformidad con la Ley 1581 de 2012 y el Decreto 1377 de 2013.

Identificación de Riesgos

Mastín Seguridad Ltda. realiza un análisis detallado de los procesos internos, sistemas tecnológicos y relaciones con terceros, identificando riesgos como:

- Acceso no autorizado a datos personales.
- Pérdida o eliminación accidental de información.
- Incumplimiento normativo por falta de controles adecuados.
- Uso indebido de información por parte de terceros.

Estos riesgos son evaluados para determinar su posible impacto en la privacidad y seguridad de los titulares de los datos.

Análisis de Riesgos

El análisis de riesgos se estructura en dos niveles:

- **Riesgo Inherente:** Representa el nivel de riesgo antes de la implementación de controles, considerando amenazas naturales o del entorno.
- **Riesgo Residual:** Es el nivel de riesgo que permanece después de aplicar medidas de mitigación, reflejando la eficacia de los controles implementados.

Se utilizarán matrices de riesgo para calcular la probabilidad e impacto de cada riesgo, permitiendo tomar decisiones informadas sobre medidas de mitigación.

Control y Mitigación de Riesgos

Mastín Seguridad Ltda. implementará controles a corto, mediano y largo plazo, incluyendo:

- **Medidas Administrativas:** Políticas internas claras y capacitación constante.
- **Medidas Tecnológicas:** Cifrado de datos, autenticación multifactor y sistemas de control de accesos.

- **Medidas Contractuales:** Cláusulas de protección de datos en contratos con terceros.
- **Protocolos de Respuesta a Incidentes:** Procedimientos para actuar ante eventos de seguridad.

Responsabilidad Demostrada

En cumplimiento del principio de responsabilidad demostrada (accountability), *Mastín Seguridad Ltda*. documentará todas las actividades relacionadas con la gestión de riesgos en la protección de datos personales, asegurando que cada proceso, desde la identificación de amenazas hasta la implementación de medidas de mitigación, esté respaldado por evidencia verificable.

Esta documentación permitirá demostrar el cumplimiento de la normativa vigente ante autoridades competentes y auditorías externas, garantizando transparencia en la gestión de la seguridad de la información. Además, se implementarán mecanismos de control y supervisión periódicos, permitiendo la mejora continua de los procedimientos y asegurando que la organización mantenga estándares elevados en la protección de datos personales.

17. Seguridad de la Información en Mastín Seguridad Ltda.

La protección de datos personales es un derecho fundamental que otorga a los titulares el control sobre su información, permitiéndoles decidir quién puede acceder a sus datos, cómo serán utilizados y para qué fines. Además, garantiza que puedan consultar, corregir, eliminar y oponerse al tratamiento de su información cuando corresponda.

La seguridad de la información se basa en tres pilares fundamentales:

- **Confidencialidad:** Garantizar que la información solo sea accesible para personas autorizadas.
- **Integridad:** Asegurar la precisión y fiabilidad de los datos, evitando alteraciones no autorizadas.
- **Disponibilidad:** Garantizar que la información esté accesible en el momento y condiciones adecuadas.

En conformidad con la **Ley 1581 de 2012**, *Mastín Seguridad Ltda*. adopta medidas de seguridad adaptadas a diversos factores, tales como:

- El riesgo inherente a la naturaleza de los datos tratados.
- El nivel de sensibilidad de la información.
- El desarrollo tecnológico disponible para protección y monitoreo.
- Las consecuencias de una posible vulneración para los titulares de los datos.
- El volumen de información manejada, asegurando su correcto tratamiento.
- Las transferencias de datos realizadas, garantizando cumplimiento normativo.

- Las experiencias previas en seguridad, aplicando mejoras continuas en los sistemas de protección.

Medidas de Seguridad en la Protección de Información Sensible

Mastín Seguridad Ltda. implementa estrictos protocolos para garantizar la protección de información sensible, controlando el acceso, almacenamiento y manejo de documentos físicos y digitales con altos estándares de seguridad.

Monitoreo con Cámaras de Seguridad.

Las áreas clave, como entradas y zonas de manejo de datos, son monitoreadas mediante cámaras de seguridad estratégicamente ubicadas.

Protección de Equipos Tecnológicos.

Mastín Seguridad Ltda. utiliza plataformas de almacenamiento en la nube, como SharePoint y Drive, para la gestión automática y segura de la información empresarial. Los accesos a estos sistemas están restringidos y protegidos mediante autenticación multifactor y protocolos de seguridad avanzados.

Gestión de Emergencias.

Se cuenta con un plan de respuesta ante emergencias como incendios o desastres naturales, que incluye rutas de evacuación, protección de documentos esenciales y extintores ubicados estratégicamente.

Inspecciones Periódicas.

Las instalaciones son revisadas frecuentemente para detectar riesgos como cerraduras dañadas, cámaras desconfiguradas o accesos no autorizados. Los hallazgos se documentan y se aplican acciones correctivas inmediatas.

Medidas de Seguridad Administrativas

Para garantizar la protección de la información sensible, *Mastín Seguridad Ltda*. implementa una serie de medidas administrativas orientadas a controlar el acceso, uso y manejo de datos personales y empresariales, asegurando el cumplimiento normativo y la mitigación de riesgos.

Políticas de Seguridad de la Información:

Se establecen normas y directrices claras sobre el manejo, almacenamiento y uso de la información, difundidas entre todo el personal y revisadas periódicamente para garantizar su actualización y cumplimiento.

Confidencialidad y Acuerdos de Privacidad:

Todo el personal con acceso a información sensible debe firmar acuerdos de confidencialidad, comprometiéndose a proteger los datos y evitar su divulgación. Esto aplica a empleados, contratistas y terceros que interactúan con la información.

Clasificación y Manejo de la Información:

Se implementan procedimientos para clasificar la información según su nivel de sensibilidad (pública, privada o confidencial), permitiendo establecer controles específicos de acuerdo con la criticidad de los datos.

Capacitación y Concienciación:

Se realizan sesiones periódicas de formación en protección de datos, ciberseguridad y buenas prácticas de manejo de información, fomentando una cultura organizacional centrada en la seguridad.

Gestión de Accesos y Roles:

Se definen y asignan roles y responsabilidades claras en el acceso a la información, asegurando que cada usuario tenga permisos únicamente sobre los datos necesarios para el desempeño de sus funciones.

Auditorías y Revisiones Periódicas:

Se ejecutan auditorías internas para identificar riesgos, verificar el cumplimiento de políticas y detectar posibles brechas de seguridad, permitiendo la implementación de mejoras continuas.

Control de Salida de Información:

Se establecen procesos de autorización y registro para la transferencia de información fuera de la organización, tanto en formato físico como digital, supervisando el uso de correos electrónicos, dispositivos portátiles y plataformas de almacenamiento en la nube.

Gestión de Incidentes:

Se cuenta con un protocolo de respuesta ante incidentes de seguridad de la información, el cual se describe en la primera parte del presente, asegurando que exista un procedimiento claro para reportar, investigar y resolver vulneraciones, minimizando impactos en la integridad de los datos.

Gestión de Incidentes y Fortalecimiento de Medidas de Seguridad

En *Mastín Seguridad Ltda.*, la protección de datos es una prioridad, por lo que se establecen medidas integrales para prevenir, detectar y responder eficazmente a incidentes de seguridad. Este capítulo describe las estrategias implementadas para fortalecer la seguridad de la información y los procedimientos adecuados en caso de una vulneración

18. Programa Integral de Gestión de Incidentes.

A pesar de las medidas preventivas, pueden ocurrir incidentes de seguridad que comprometan la integridad de los datos. Para ello, *Mastín Seguridad Ltda*. ha desarrollado un programa de gestión de incidentes con procedimientos claros y estructurados.

Identificación y Registro de Incidentes

La detección temprana de incidentes es esencial para minimizar daños. Se han establecido procedimientos formales y tecnológicos que permiten la rápida identificación y registro de eventos de seguridad.

Todos los incidentes son clasificados según su naturaleza, ya sean accesos no autorizados, pérdida de información, alteraciones de datos o vulneraciones externas, permitiendo una mejor gestión del riesgo.

Evaluación de Impacto

Ante un incidente, es necesario evaluar su impacto para tomar acciones adecuadas. Para ello, se realizan análisis basados en criterios específicos:

- Confidencialidad: Se determina si la filtración de datos compromete la privacidad de los titulares.
- Integridad: Se analiza si la información ha sido modificada de manera indebida.
- Disponibilidad: Se mide el tiempo de recuperación del sistema y el impacto en la continuidad de las operaciones.

A partir de esta evaluación, se elabora un informe detallado, con recomendaciones iniciales para mitigar daños y restaurar la seguridad del sistema.

Acciones Correctivas

Para abordar los incidentes de seguridad, *Mastín Seguridad Ltda*. aplica medidas de recuperación y prevención que permiten restablecer la información y evitar futuras vulneraciones.

Entre las principales acciones correctivas se encuentra el restablecimiento de copias de seguridad actualizadas, asegurando la recuperación eficiente de datos afectados. Asimismo, se refuerzan los controles de seguridad, implementando autenticación multifactorial y cifrado avanzado para evitar accesos indebidos.

Se realiza una revisión y actualización de configuraciones críticas de software y hardware, con el fin de eliminar posibles puntos de vulnerabilidad.

De igual manera, el personal recibe capacitaciones específicas sobre gestión de incidentes, para que pueda responder de manera eficiente ante cualquier eventualidad.

Por último, se llevan a cabo auditorías post-incidente, verificando la efectividad de las medidas implementadas y ajustando procesos según las necesidades detectadas.

19. Notificación Obligatoria

Para cumplir con la normativa vigente, *Mastín Seguridad Ltda*. ha definido procedimientos claros de notificación de incidentes tanto a entidades reguladoras como a los titulares de los datos.

- Notificación Interna: Se reporta inmediatamente el incidente al Oficial de Protección de Datos (DPO) y al equipo de TI, asegurando una rápida respuesta.
- Notificación a la Superintendencia de Industria y Comercio: Se envía un informe detallado del incidente, incluyendo su naturaleza, alcance, medidas correctivas y posibles consecuencias.
- Notificación a los Titulares de Datos: Se informa a los afectados sobre el impacto del incidente y las medidas que pueden adoptar para proteger su información. La empresa proporciona un canal de comunicación para aclarar dudas y brindar soporte.

20. Sistema de Monitoreo Continuo

Para garantizar la eficacia de las medidas de seguridad, *Mastín Seguridad Ltda*. ha establecido un sistema de monitoreo continuo, que permite verificar la correcta implementación de controles y detectar posibles riesgos antes de que se conviertan en amenazas.

Revisión y Mejora Continua

Conscientes de que las amenazas evolucionan constantemente, *Mastín Seguridad Ltda*. se compromete a actualizar periódicamente sus políticas y procedimientos, alineándolos con nuevos requerimientos normativos y avances tecnológicos.

Asimismo, se realizan análisis comparativos con mejores prácticas del sector, permitiendo la optimización de estrategias de seguridad.

Se fomenta la innovación en técnicas de protección de datos, incorporando nuevas herramientas y metodologías que refuercen la seguridad de la información.

Responsabilidades

La implementación y supervisión de este programa estará a cargo del área de seguridad de la información, bajo la dirección del Oficial de Protección de Datos.Este equipo es responsable de: Garantizar el cumplimiento de las medidas de seguridad, atender inquietudes sobre el manejo de información, reportar incidentes ante las autoridades competentes.

21. Modificación de las Políticas

Mastín Seguridad Ltda. se reserva el derecho de modificar en cualquier momento su Política de Tratamiento y Protección de Datos Personales, con el objetivo de ajustarla a nuevas normativas, requerimientos operativos o mejoras en la gestión de la información.

Cualquier modificación será comunicada oportunamente a los titulares de los datos mediante los canales de contacto habituales, asegurando un plazo de diez (10) días hábiles antes de su entrada en vigor.

En caso de que un titular no esté de acuerdo con los cambios realizados, ya sean generales o específicos, y cuente con razones válidas que justifiquen su decisión de no continuar con la autorización para el tratamiento de sus datos personales, podrá solicitar el retiro de su información mediante correo electrónico a info@alzateyasociados.com o sarlaft@mastinseguridad.com.

Sin embargo, los titulares no podrán solicitar la eliminación de sus datos si *Mastín Seguridad Ltda*. tiene un deber legal o contractual de continuar con su tratamiento.

Sanciones por Infracciones a la Política de Protección de Datos Personales
El incumplimiento de esta Política de Protección de Datos Personales, así como de la normativa vigente, podrá generar acciones disciplinarias y legales que pueden derivar en la rescisión inmediata de relaciones contractuales o comerciales en los siguientes casos:

Relaciones Laborales

Si un empleado incurre en faltas graves respecto a la protección de datos personales, *Mastín Seguridad Ltda*.podrá dar por terminado el contrato laboral por justa causa, conforme al reglamento interno de trabajo y las disposiciones del Código Sustantivo del Trabajo.

Acuerdos Comerciales o Civiles

Cuando un contratista, proveedor u otra parte vinculada mediante acuerdos comerciales o civiles incumpla las directrices de esta política, la empresa podrá finalizar el contrato, previa notificación, de acuerdo con los términos establecidos en el acuerdo contractual y la legislación aplicable.

22. Obligaciones Adicionales

Además de la terminación contractual, las personas o entidades que incurran en incumplimientos pueden enfrentar acciones legales, que incluyen demandas civiles o denuncias penales para la reparación de los daños causados a los titulares de los datos personales.

Mastín Seguridad Ltda. se reserva el derecho de adoptar medidas correctivas y legales frente a cualquier infracción detectada, con el propósito de proteger los derechos de los titulares y asegurar el cumplimiento de la normativa vigente en materia de protección de datos personales.

TABLA: GESTIÓN DE BASES DE DATOS, MEDIDAS DE SEGURIDAD Y RESPONSABILIDAD DEMOSTRADA EN MASTÍN SEGURIDAD LTDA.

Base de Datos	Tipos de Datos Recolectados	Encargado interno	Nivel de Seguridad	Medidas de Seguridad (Técnicas y Administrativas)	Documentos Soporte
Empleados	Sensibles (salud, biométricos), privados (contratos, pagos), semiprivados (contacto)	**Talento Humano**	**Alto**	Autenticación multifactor, acceso restringido, cifrado en SharePoint y OneDrive, auditoría anual, cambio de contraseñas, capacitación anual e inducción	Acuerdos de confidencialidad, autorización de tratamiento de datos, contratos laborales
Clientes	Privados (contratos, pagos), semiprivados (contacto), públicos (razón social)	**Comercial**	**Medio**	Encriptación de datos, control de accesos, monitoreo de actividad en plataformas digitales, auditoría anual, capacitación anual	Acuerdos comerciales, términos y condiciones de servicio, autorización de datos
Proveedores	Privados (contratos, cuentas bancarias), semiprivados (contacto), públicos	**Administración**	**Medio**	Almacenamiento seguro en la nube, gestión de accesos digitales, auditoría anual,	Contratos de prestación de servicios, acuerdos de privacidad, registros de proveedores

Base de Datos	Tipos de Datos Recolectados	Encargado interno	Nivel de Seguridad	Medidas de Seguridad (Técnicas y Administrativas)	Documentos Soporte
	(razón social, NIT)			capacitación en protección de datos	
Videovigilancia	Sensibles (imágenes captadas en zonas monitoreadas), semiprivados (registro de actividad en acceso)	**Operaciones**	**Alto**	Almacenamiento en servidores seguros, restricción de acceso por credenciales, auditoría anual, revisión periódica de grabaciones	Autorizaciones de videovigilancia, políticas de privacidad en monitoreo
Socios	Privados (datos financieros), semiprivados (datos de contacto)	**Gobierno Corporativo**	**Alto**	Autenticación segura, revisión periódica de accesos, auditoría anual, capacitación anual en seguridad financiera	Acuerdos societarios, documentos de inversión, contratos de confidencialidad
Seguridad y Salud en el Trabajo	Sensibles (datos médicos y de riesgos laborales), semiprivado	**SIG**	**Alto**	Acceso restringido, auditoría anual, capacitación	Historia laboral de riesgos, registros de seguridad en el trabajo

Base de Datos	Tipos de Datos Recolectados	Encargado interno	Nivel de Seguridad	Medidas de Seguridad (Técnicas y Administrativas)	Documentos Soporte
	s (registros de salud ocupacional)			en seguridad laboral	
Cartera	Privados (información de pagos, cuentas), semiprivados (contacto)	**Contabilidad**	**Medio**	Protección contra accesos no autorizados, cifrado de datos financieros, auditoría anual, cambios de contraseña según las políticas imternas	Registros de pagos, acuerdos de cobro, documentos contractuales
Aspirantes	Privados (hojas de vida, evaluaciones), semiprivados (contacto, referencias)	**Selección**	**Medio**	Seguridad en almacenamiento, auditoría anual, capacitación en manejo de datos personales	Consentimiento informado, bases de datos de selección, acuerdos de privacidad
Aprendices	Privados (contratos de aprendizaje), semiprivados	**Talento Humano**	**Medio**	Registro y control digital de acceso, almacenamiento en SharePoint y Drive,	Convenios de aprendizaje, registros de formación, políticas internas

Base de Datos	Tipos de Datos Recolectados	Encargado interno	Nivel de Seguridad	Medidas de Seguridad (Técnicas y Administrativas)	Documentos Soporte
	(información académica)			auditoría anual, capacitación anual	
Convenios	Privados (documentación contractual), públicos (entidades aliadas)	**Administración**	**Medio**	Control de acceso digital, auditoría de movimientos en sistemas, auditoría anual, revisión contractual periódica	Acuerdos de cooperación, contratos de convenios, registros de colaboración
Archivos Inactivos	Privados (expedientes antiguos), semiprivados (datos históricos)	**Administración**	**Medio**	Cifrado de documentos, auditoría anual sobre cumplimiento	Registro de eliminación de archivos, política de conservación
Visitantes	Semiprivados (registro de ingreso), públicos (razón social en caso de empresas); sensibles (huellas, imagen)	Operaciones	Alto	Control de acceso digital, registro en sistemas de seguridad, auditoría anual sobre accesos	Políticas de seguridad de acceso, protocolos de privacidad de visitantes

Aspectos Clave:

- Las auditorías se realizan mínimo una vez al año, además de auditorías extraordinarias ante cambios significativos.
- Las capacitaciones en seguridad de la información se realizan al menos una vez al año y en la inducción del personal.

Control de cambios			
Descripción del cambio	**Versión**	**Fecha**	**Responsable y cargo**
Creación	1	19/09/2025	Mateo Ramos – Oficial de PDP

ELABORO/MODIFICO	**REVISÓ**	**APROBÓ**
Nombre: Mateo Ramos Cargo: Oficial de PDP	Nombre: María Carolina Rodríguez Cargo: Directora Administrativa	Nombre: Rodolfo Tamayo Cargo: Gerente General