	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

POLÍTICA DE TRATAMIENTO DE DATOS – SEGURIDAD DISSEL LTDA.

1. Introducción

Seguridad Dissel Ltda., desarrollando actividades vinculadas al sector de vigilancia y seguridad privada, y en cumplimiento a su objeto social, reconocen la especial relevancia que tiene la protección de los datos personales en el marco de la prestación de servicios de seguridad, control, prevención del riesgo y protección de personas, bienes e instalaciones.

En razón a la naturaleza propias del sector, la organización realiza el tratamiento de datos personales de clientes, colaboradores, contratistas, proveedores, visitantes y terceros, incluyendo información recolectada a través de sistemas de videovigilancia, controles de acceso, registros operativos, plataformas tecnológicas y canales digitales, lo cual exige la adopción de medidas reforzadas de seguridad y confidencialidad.

Por lo anterior, la empresa adopta la presente Política de Tratamiento de Datos Personales, con el fin de garantizar el cumplimiento de la Ley Estatutaria 1581 de 2012, el Decreto 1377 de 2013, el Decreto 1074 de 2015, así como los lineamientos de la Superintendencia de Industria y Comercio – SIC, y demás normas aplicables al sector de vigilancia y seguridad privada, asegurando el respeto por el derecho fundamental de hábeas data.

2. Objetivo


La presente política tiene como objetivo establecer los lineamientos, procedimientos y medidas técnicas, administrativas y jurídicas que regulan el tratamiento de los datos personales que Seguridad Dissel Ltda., recolectan, tratan, almacenan, circulan, transmiten, transfieren o suprimen, en desarrollo de las actividades propias del servicio de vigilancia y seguridad privada.

2.1. Objetivos específicos

- Garantizar que el tratamiento de datos personales se realice de manera lícita, proporcional, necesaria y acorde con las finalidades de la actividad comercial de la empresa.
- Proteger la información personal tratada en el marco de operaciones de control, monitoreo, prevención del delito y gestión del riesgo.
- Establecer reglas claras para la circulación restringida de los datos, en atención al carácter sensible y estratégico de ciertos datos tratados en el sector.
- Asegurar la transparencia frente a los titulares respecto de las finalidades, derechos y mecanismos de atención.
- Cumplir las obligaciones legales, regulatorios y contractuales aplicables al sector de vigilancia y seguridad privada.

3. Alcance

La presente política aplica a todos los datos personales que sean objeto de tratamiento por parte de Seguridad Dissel Ltda., en su condición de responsable del tratamiento. La política se concentra en el tratamiento de los datos personales de: a) Clientes y potenciales de los servicios de vigilancia y seguridad privada; b) Colaboradores, guardas de seguridad, supervisores, personal

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

administrativo y aspirantes; c) Proveedores, contratistas, aliados estratégicos y subcontratistas; d) Visitantes y terceros que ingresen a instalaciones protegidas o vigiladas; e) Usuarios de plataformas digitales, aplicativos, sistemas de control y canales electrónicos de atención, entre otros. Incluye, datos recolectados mediante: (i) Sistemas de videovigilancia, cámaras corporales y centros de monitoreo. (ii) Controles de acceso físico y electrónico. (iii) Registros operativos, bitácoras de servicio y reportes de novedad. (iv) Formularios físico o digitales, correos electrónicos y plataformas tecnológicas; entre otras.

4. Marco normativo

Seguridad Dissel Ltda. cumple con la normatividad del tratamiento de datos, Ley 1581 de 2012 y Decreto 1337 de 2013, así como las sugerencias y lineamientos de la Superintendencia de Industria y Comercio y, demás normas concordantes.


Deberes de Seguridad Dissel Ltda. como encargado del tratamiento de datos personales.

- Realizar el tratamiento de los datos personales únicamente conforme a las instrucciones impartidas por el responsable del tratamiento, y de acuerdo con las finalidades autorizadas, la ley y los contratos suscritos.
- Garantizar al titular, en todo momento, el pleno y efectivo ejercicio del derecho de hábeas data, en los términos establecidos por la normatividad vigente.
- Conservar la información personal bajo condiciones de seguridad técnicas, humanas y administrativas adecuadas, que impidan su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Abstenerse de utilizar los datos personales para finalidades distintas a las autorizadas por el responsable o las previstas en la ley.
- Mantener la confidencialidad de los datos personales tratados, incluso después de finalizada la relación contractual con el responsable del tratamiento.
- Actualizar, rectificar o suprimir lo datos personales cuando así lo indique el responsable del tratamiento, o cuando resulte procedente conforme a la ley.
- Informar oportunamente al responsable del tratamiento sobre cualquier incidente de seguridad, violación a los códigos de seguridad o riesgo en la administración de la información personal que pueda afectar a los titulares.
- Tramitar las consultas y reclamos presentados por los titulares, cuando le corresponda, de conformidad con los procedimientos y términos establecidos en la ley 1581 de 2012 y demás normas aplicables.
- Cumplir las instrucciones, requerimientos y directrices impartidas por la Superintendencia de Industria y Comercio, en su calidad de autoridad nacional de protección de datos personales.

5. Tratamiento de datos sensibles

De conformidad con lo establecido en la ley 1581 de 2012, el Decreto 1074 de 2015 y demás normas aplicables, SEGURIDAD DISSEL LTDA. aplicará las limitaciones legales al tratamiento de datos sensibles, verificando que:

- El titular haya otorgado su autorización explícita y previa, salvo en los casos en que la ley exceptué dicho requisito.

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

- El tratamiento sea necesario para salvaguardar los derechos fundamentales del titular y este se encuentre incapacitado.
- El tratamiento sea indispensable para el reconocimiento, ejercicio o defensa o de un derecho en un proceso judicial o administrativo.
- El tratamiento tenga una finalidad histórica, estadística o científica, aplicando en estos casos medidas de anonimización de la información.

Así mismo, SEGURIDAD DISSEL LTDA, implementará medidas técnicas, humanas y administrativas que garanticen la confidencialidad y seguridad de la información de los titulares, especialmente cuando los datos provengan de sistemas de videovigilancia, biometría o inteligencia artificial (IA), utilizados para la prestación de los servicios de seguridad privada, sistemas de videovigilancia y monitoreo de alarmas.

5.1. Finalidades del tratamiento de datos sensibles

La recolección de datos personales sensibles de titulares de la empresa SEGURIDAD DISSEL LTDA. tienen las finalidades que se especifican para cada caso.

Tipo de dato	Finalidad
Datos relativos a la salud	<ul style="list-style-type: none"> ● Trámite de incapacidades de los trabajadores de la empresa. ● Documentos de carácter médico como incapacidades, epicrisis, resultados diagnósticos, pruebas de laboratorio, así como cualquier otro dato de carácter reservado que entregue el colaborador. ● Cumplir con el Sistema de Seguridad y Salud en el Trabajo. ● Exámenes ocupacionales de ingreso, periódico y egreso del trabajador. ● Prevención, control y seguimiento de las condiciones de salud de los trabajadores. ● Evaluar condiciones de aptitud psicofísica requeridas por el porte de armas o desempeño de funciones de riesgo, conforme al Decreto 356 de 1994, normas del MinDefensa y Superintendencia de Vigilancia y Seguridad Privada. ● Implementar programas de promoción y prevención en salud ocupacional, vacunación, ergonomía, vigilancia epidemiológica y hábitos saludables.
Datos relativos al origen racial, étnico, orientación sexual, identidad de género, orientación política, convicciones	<ul style="list-style-type: none"> ● Para fines estadísticos, caracterización, protección y tratamiento. ● Cumplir con la política de equidad de género y protección a personas en estado de vulnerabilidad.




SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST

COD: OD-DE-10

POLÍTICA TRATAMIENTO DE DATOS

VERSION: 1

<p>religiosas o filosóficas.</p>	<ul style="list-style-type: none"> ● Cumplir con el Sistema de Seguridad y Salud en el Trabajo. ● Llevar a cabo intervenciones donde que evidencien la discriminación o acoso por las condiciones del colaborador. ● Promover un entorno laboral inclusivo y libre de discriminación, mediante la adopción de protocolos internos de trato digno y enfoque diferencial.
<p>Datos capturados por sistema de video vigilancia, alarmas e IA</p>	<ul style="list-style-type: none"> ● Cumplir con la política de video vigilancia ● Seguridad pública, vial, laboral, contractual y de entornos, así como bienes de la empresa. ● Usar para fines de cumplimiento de las obligaciones del Reglamento Interno de Trabajo. ● Cumplir con el Sistema de Seguridad y Salud en el Trabajo. ● Prevenir delitos, facilitar, colaborar y apoyar con las autoridades competentes. ● Proteger de actos de discriminación, acoso laboral entre los colaboradores de la empresa. ● Verificar el inventario en le cargue y descargue de mercancías, condiciones óptimas de recibido, estado, despacho y uso de medidas de seguridad. ● Supervisar el cumplimiento del Reglamento Interno de Trabajo, políticas internas y contrato individual de trabajo. ● Optimizar la respuesta ante eventos de riesgo, activando protocolos automáticos de alarma, notificación o registro en tiempo real. ● Apoyar procesos de investigación interna o auditoría, cuando se requiera verificar los hechos de seguridad, pérdida, daño o incumplimiento de protocolos.
<p>Datos biométricos, imágenes, voz, fotografías, videograbaciones, huellas dactilares y audios.</p>	<ul style="list-style-type: none"> ● Identificar los colaboradores. ● Campañas de mercadeo, corporativa y/o comercial. ● Evidenciar las actividades, eventos, carnetización. ● Evidencia de control y auditoria. ● Publicación en redes sociales, campañas promocionales y publicidad. ● Cumplir las obligaciones contractuales. ● Registrar y verificar asistencia o control horario mediante sistemas biométricos autorizados, en reemplazo de métodos manuales de control.


	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

	<ul style="list-style-type: none"> ● Asegurar autenticación y trazabilidad digital en el uso de sistemas de información, cámaras o dispositivos con acceso restringido. ● Validar identidad en procesos de investigación o reporte de incidentes.
Personas en condición de discapacidad	<ul style="list-style-type: none"> ● Cumplir con el Sistema de Gestión de Seguridad y Salud en el Trabajo. ● Facilitar la atención de servicios de salud y prevención del riesgo. ● Facilitar la accesibilidad de documentos solicitados a la empresa. <p>Así como, todas aquellas expresadas en el segmento Nro. 1 de la presente política de tratamiento de datos.</p>
Población vulnerable	<ul style="list-style-type: none"> ● Análisis sociodemográfico, estadísticas e históricos. ● Cumplir con el Sistema de Gestión de Seguridad y Salud en el Trabajo. ● Registrar madres cabeza de familia o trabajadores en condición de vulnerabilidad para prevención de acoso laboral y tratamiento especial de acuerdo con su condición. <p>Así como, todas aquellas expresadas en el segmento Nro. 1 de la presente política de tratamiento de datos.</p>

5.2. Finalidades de tratamiento de datos sensibles para externos y clientes.

Captar, procesar, almacenar y conservar imágenes, audios o cualquier registro proveniente de los sistemas de videovigilancia o monitoreo instalados en los bienes, inmuebles o áreas de responsabilidad del cliente, con el fin de prevenir, detectar, verificar o reaccionar ante situaciones de riesgo, alarma o amenaza.

- Garantizar la continuidad, confiabilidad y trazabilidad de los servicios contratados, incluyendo la verificación de eventos, la confirmación de incidentes, alarmas y la **entrega de reportes de seguridad**.
- Cumplir las obligaciones establecidas en los contratos suscritos entre SEGURIDAD DISSEL LTDA, y sus clientes, así como las disposiciones emitidas por la Superintendencia de Vigilancia y Seguridad Privada, Policía Nacional o las autoridades judiciales y administrativas competentes.
- Registrar y analizar los datos obtenidos por los sistemas de alarma, sensores, dispositivos de control perimetral, portería eléctrica y demás medios electrónicos para detectar intrusiones, accesos no autorizados o anomalías operativas.
- Gestionar la activación de protocolos de respuesta inmediata, contacto con autoridades, y acciones preventivas o reactivas, en atención a la alerta generada por los equipos instalados.

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1


- Proveer trazabilidad de los eventos captados generando bitácoras, reportes de auditoría y respaldos digitales cifrados, que permitan documentar las actuaciones de vigilancia o reacción ante incidentes.
- Utilizar sistemas de analítica de video con inteligencia artificial para la detección automatizada de movimientos, aglomeraciones, intrusiones, comportamientos sospechosos o situaciones anómalas, dentro de los parámetros técnicos definidos en el contrato y bajo estrictos protocolos de confidencialidad.
- Emplear la información procesada por la IA con fines de seguridad preventiva, verificación de incidentes o mejora del servicio.
- Mantener los registros en entornos seguros, con controles de acceso, cifrado, anonimización y políticas de retención y eliminación de datos acordes con la naturaleza del servicio y las disposiciones de la SIC.
- Suministrar la información, grabaciones o reportes que sean solicitados por los clientes contratantes, previa verificación de legitimación o titularidad del inmueble o sistema monitoreado.
- Colaborar con autoridades judiciales, de policía o administrativas que requieran datos o grabaciones en el marco de una investigación o actuación legal.
- Almacenar los datos sensibles obtenidos a través de sistemas de videovigilancia y alarmas en infraestructuras tecnológicas seguras, con acceso restringido a personal autorizado y en cumplimiento de las normas de seguridad de la información y ciberseguridad.
- Monitorear, detectar y registrar situaciones que puedan representar amenazas para la seguridad pública, privada o empresarial, activando protocolos de respuesta y alertando a las autoridades competentes.
- Proteger la integridad física de personas, bienes e instalaciones ubicadas dentro del rango de acción de los sistemas implementados por la empresa.
- Apoyar las investigaciones internas o externas sobre eventos de pérdida, daño, hurto o alteración de bienes, así como otros delitos o comportamientos ilícitos garantizando el manejo responsable de la evidencia.

5.3. Derechos de los niños, niñas y adolescentes

Para el tratamiento de datos personas de niños, niñas y adolescentes, se respetarán sus derechos fundamentales, así como garantizará que la información sea utilizada respondiendo a las disposiciones estipuladas en la ley 1581 de 2012 y en el Decreto 1337 de 2013, así:

- Que respondan y respeten el interés superior de los niños, niñas y adolescentes.
- Que se asegure del respeto de los derechos fundamentales.

Cumplido los anteriores requisitos, el representante legal de los niños, niñas o adolescentes otorgará la autorización, previo ejercicio del menor de su derecho de ser escuchado, opinión que serpa valorada teniendo en cuenta la madurez, autonomía y capacidad para atender el asunto.

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

6. Tratamiento de datos de personas en condición de discapacidad y su registro de acuerdo con la resolución 0312 de 2019 “por la cual se definen los Estándares mínimos del Sistema de Gestión de la Seguridad y Salud en el Trabajo SG-SST”

6.1. De los datos sensibles de las personas en condición de discapacidad y población vulnerable.

En el desarrollo de las actividades propias de **SEGURIDAD DISSEL LTDA.**, el tratamiento de los datos personales y datos sensibles de trabajadores, contratistas, visitantes, clientes y demás titulares en condición de discapacidad o situación de vulnerabilidad se realizará conforme a los principios de legalidad, fidelidad, libertad, veracidad, transparencia, seguridad, confidencialidad y accesibilidad establecidos en la ley 1581 de 2012, la ley 1618 de 2013, la Convención sobre los Derechos de las personas con Discapacidad, ley 1346 de 2009 y la Resolución 0312 de 2019 del SG-SST.

Este segmento establece las reglas específicas para la recolección, almacenamiento, uso, circulación y supresión de dicha información.

6.2. Definiciones

Personas en condición de discapacidad: Son aquellas personas que presentan deficiencias físicas, mentales, intelectuales o sensoriales a largo plazo que, al interactuar con el entorno, encuentran diversas barreras, que pueden impedir su participación plena y efectiva en la sociedad, en igualdad de condiciones con los demás ciudadanos. (Convención de la ONU, 2006, Clasificación Internacional del Funcionamiento, la Discapacidad y la salud, OMS, 2002).

Población vulnerable: Grupo de personas que se encuentran en estado de desprotección o incapacidad frente a una amenaza a su condición psicológica, física y mental, entre otras. (Ministerio de Educación Nacional de Colombia)

6.3. Finalidades

El tratamiento de los datos de las personas en condición de discapacidad y población vulnerable tendrán las finalidades que se especifican para cada caso, las cuales se encuentran alienadas a las exigencias de la resolución 0312 de 2019 “por la cual se definen los estándares mínimos de Gestión de la Seguridad y Salud en el Trabajo SG-SST”.

Titular del dato	Finalidad
Personas en condición de discapacidad	<ul style="list-style-type: none"> ● Cumplir con el adecuado tratamiento de datos para el cumplimiento del ítem de la resolución 0312 de 2019 en su artículo 16, ítem 23 sobre la “Descripción sociodemográfica y diagnóstico de las condiciones de salud de los trabajadores” ● Generar mayor facilidad en la atención de servicios de salud a quienes entren en las instalaciones de la empresa o aquellos trabajadores, contratistas o colaboradores de la empresa, así como la prevención del riesgo.




SISTEMA INTEGRADO DE GESTION
CALIDAD-CONTROL Y SEGURIDAD-SST

COD: OD-DE-10

POLÍTICA TRATAMIENTO DE DATOS

VERSION: 1

	<ul style="list-style-type: none">● Facilidad en la accesibilidad a los documentos solicitados por la empresa a través de diferentes herramientas para la lectura de los mismos como formato de texto, audio o presentación ampliada.● Realizar procesos de prevención de riesgos, gestión de emergencias, evacuación y atención prioritaria conforme a las obligaciones del SG-SST.● Implementar acciones de reubicación laboral, adaptación del puesto y ajustes razonables según las restricciones médicas permanentes o temporales del titular, garantizando condiciones de seguridad, salud y prevención del riesgo.● Realizar seguimiento a las condiciones de salud, evolución de incapacidades, recomendaciones médicas y riesgos asociados al desempeño de funciones, con el fin de prevenir agravamiento de la condición y garantizar su protección reforzada.● Identificar riesgos críticos para evitar la asignación de tareas incompatibles con la condición de trabajador y prevenir situaciones que puedan comprometer su integridad física o la de terceros.● Gestionar las obligaciones legales relacionadas con la estabilidad laboral reforzada, evaluando condiciones de permanencia, reubicación y continuidad conforme a la ley 361 de 1997 y la jurisprudencia constitucional.● Conservar y suministrar, cuando proceda, la información estrictamente necesaria a la ARL, EPS, Min Trabajo u otras entidades competentes para la verificación de obligaciones en materia de seguridad y salud en el trabajo.● Incorporar información relevante para la atención en emergencias, evacuación asistida y planes de contingencia, garantizando el apoyo oportuno en situaciones de riesgo.
Población vulnerable	<ul style="list-style-type: none">● Cumplir con los análisis sociodemográficos exigidos por la Resolución 0312 de 2019, incluyendo ubicación geográfica, contextos culturales, zonas de riesgo, tiempos de desplazamiento y otros factores que inciden en la gestión del riesgo laboral.● Registrar información diferencial de vulnerabilidad que permita identificar riesgos psicosociales y prevenir situaciones de acoso laboral o discriminación.● Facilitar la implementación de medidas preventivas, acciones afirmativas y apoyos diferenciados dentro del SG-.SST.● Recolectar y analizar información relacionada con ubicación geográfica, contextos sociales, zonas de

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

	<p>riesgo, trayectos, condiciones del entorno y demás factores que inciden en la seguridad del trabajador.</p> <ul style="list-style-type: none"> ● Diseñar y aplicar acciones afirmativas, ajustes razonables, adaptaciones operativas y apoyos proporcionales para asegurar la permanencia laboral, la inclusión, la accesibilidad y la participación en igualdad de condiciones. ● Registrar y evaluar condiciones de vulnerabilidad para identificar riesgos psicosociales, prevenir situaciones de acoso laboral o discriminación, y orientar decisiones que garanticen la protección especial del titular. ● Incorporar información necesaria para priorizar a personas vulnerables en planes de emergencia, evacuación y contingencias, y suministrar, exclusivamente cuando la ley lo permita, los datos mínimos indispensables a EPS, ARL, MinTrabajo u otras entidades encargadas de garantizar la protección del titular.
--	---

6.4. Herramientas para el acceso a los datos personales de las personas en condición de discapacidad.

El responsable del tratamiento de datos adoptará las siguientes medidas adicionales para las personas en condición de discapacidad, cumpliendo con ello con los principios de la ley 1581 de 2012, mecanismos razonables de accesibilidad comunicacional.

Accesibilidad: El responsable facilitará el acceso a la información sobre el tratamiento de los datos personales y datos sensibles, utilizando formatos accesibles y proporcionando los medios necesarios para que puedan conocer sus derechos y las finalidades del tratamiento de los datos, como los siguientes.

Texto: El responsable proporcionará la política de tratamiento de datos en un formato simple y legible, utilizando un tamaño adecuado o acorde a la necesidad y colores que permitan su visualización.


Audio: Para aquellas personas en condición de discapacidad con limitaciones a la visión, ofrecerá audio-texto, o de manera directa informará y/o guiará sobre los apartados a conocer por el titular.

Estas medidas se implementan de manera proporcional y razonable, buscando asegurar la igualdad de condiciones, no discriminación y participación plena de los titulares.

Tratamiento de información que no requiere autorización del titular

De conformidad con lo dispuesto en el artículo 10 de la ley 1581 de 2012, Seguridad Dissel Ltda., informa que no será necesaria la autorización previa, expresa e informada por el titular para el tratamiento de datos personales cuando dicho tratamiento se encuentre amparado por alguna de las excepciones previstas en la ley.

6.5. Ámbito de aplicación

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

El presente aplica a todos los titulares de datos personales cuya información sea objeto de tratamiento por parte de Seguridad Dissel Ltda., independientemente de su calidad o vínculo con la empresa, siempre que el tratamiento se encuentre comprendido dentro de las excepciones legales que no requieren autorización. Este tratamiento podrá realizarse en el marco del desarrollo del objeto social, el cumplimiento de las obligaciones legales y regulatorias, la atención de requerimientos de autoridades competentes, y la garantía de la seguridad física, operativa, jurídica y tecnológica de la organización.

6.6. Definiciones

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

Dato público: Es el dato que no es semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio, a su calidad de comerciante o de servidor público, y aquellos que puedan obtenerse sin reserva alguna.

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

6.7. Recolección de datos personales

Seguridad Dissel Ltda. podrá recolectar datos personales sin autorización del titular cuando:


- La información sea requerida por una autoridad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Los datos correspondan a información de naturaleza pública.
- Exista una situación de urgencia médica o sanitaria que haga indispensable el tratamiento.
- El tratamiento esté expresamente autorizado por ley para fines históricos, estadísticos o científicos.
- Se trate de datos relacionados con el registro civil de las personas.

La recolección podrá realizarse a través de medios físicos o digitales, sistema de información, registros, documentos públicos, bases de datos de acceso permitido, sistemas de videovigilancia, controles de acceso u otros mecanismos legítimos.

6.8. Finalidades del tratamiento de los datos personales

El tratamiento de datos personales que no requiere autorización del titular se realizará, entre otras, para las siguientes finalidades generales:

- Cumplir obligaciones legales, regulatorias, contractuales y estatutarias.
- Atender requerimiento de autoridades judiciales, administrativas o de control. Garantizar la seguridad de las personas, bienes, instalaciones y sistemas de información.
- Prevenir, detectar e investigar incidentes, riesgos o eventos que afecten la seguridad física o tecnológica.
- Administrar y conservar registros exigidos por la ley.
- Desarrollar actividades con fines históricos, estadísticos o científicos autorizados por la ley.
- Atender situaciones de urgencia o sanitaria.

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

- Operación de sistemas de videovigilancia para la captación, grabación, almacenamiento y análisis de imágenes y videos obtenidos mediante sistemas de CCTV, cámaras corporales, centros de monitoreo y demás dispositivos de seguridad, con el fin de prevenir actos delictivos, proteger la integridad de las personas, preservar los bienes y apoyar investigaciones internas o requerimientos de autoridades competentes.
- Control de accesos y verificación de identidad para el registro y verificación de ingreso y salida de personas, vehículos y activos en instalaciones vigiladas, áreas restringidas o zonas críticas, mediante listas de control, registros manuales o electrónicos, sistemas biométricos, tarjetas de acceso o mecanismo similares, cuando sea necesario para garantizar la seguridad.
- Gestión de incidentes, eventos de seguridad y evidencia, para la recolección, análisis y conservación de información relacionada con incidentes de seguridad, novedades operativas, reportes de alarmas, registro de rondas, bitácoras, evidencias físicas o digitales y demás datos necesarios para la prevención, investigación, documentación y reporte de eventos que puedan afectar la seguridad.
- Atención de emergencias y coordinación con autoridades, para el suministro de información a organismos de socorro, autoridades judiciales, policiales o administrativas, en situaciones de emergencia, riesgo inminente, alteración del orden público o hechos que comprometan la vida, integridad o seguridad de las personas o bienes.

7. Visitantes y usuarios de la página web


Seguridad Dissel Ltda. con el fin de establecer las reglas aplicables al tratamiento de la información personal recolectada a través de su página web, portales digitales y demás canales virtuales dispuestos para la interacción con visitantes y usuarios. El tratamiento de los datos se realizará conforme a la legislación vigente, garantizando el respeto y garantía de los derechos de los titulares y la adopción de medidas adecuadas para el uso responsable, seguro y transparente de la información en entornos digitales.

7.1. Ámbito de aplicación

El presente segmento aplica a todas las personas naturales que, en calidad de:

- Visitantes de la página web institucional.
- Usuarios de portales web, plataformas digitales o aplicativos administrados por la empresa.
- Personas que diligencien formularios de contacto, inscripción, registro, solicitudes de información o cotización.
- Usuarios que interactúen con los contenidos digitales, canales de atención virtual o herramientas de comunicación electrónica.

Cuyos datos personales sean recolectados, almacenados, usados, circulados o suprimidos por Seguridad Dissel Ltda., a través de medios digitales o electrónicos. El tratamiento de los datos personales en entornos digitales podrá incluir el uso de cookies, tecnologías similares o herramientas de analítica, de conformidad con la Política de tratamiento de cookies adoptada por la empresa, la cual regula de manera específica su uso, finalidades, tipos de cookies empleadas y los mecanismos para que los usuarios gestionen sus preferencias, sin perjuicio de la aplicación integral.

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

8. Recolección de datos personales en medios digitales.

Seguridad Dissel Ltda., podrá recolectar datos personales de visitantes y usuarios de la página web a través de:


- Formularios de contacto, inscripción o registro.
- Solicitudes de información, cotizaciones o demostraciones de servicios.
- Canales de atención virtual, chatbots o correos electrónicos.
- Sistemas de analítica web y métricas de navegación.
- Registros de interacción con contenidos digitales.
- Cookies técnicas, analíticas o funcionales, conforme a la política de cookies adoptada por la empresa.

La recolección se realizará mediante plataformas tecnológicas seguras, adoptando medidas razonables para garantizar la integridad, confidencialidad y disponibilidad de la información.

8.1. Finalidades del tratamiento de los datos personales

Los datos de los visitantes y usuarios de la página web serán tratados, de manera enunciativa y no limitativa, para las siguientes finalidades:

- a) Atención de solicitudes e interacción digital.
 - Atender consultas, inquietudes, solicitudes de información o requerimientos presentados a través de la página web o portales digitales.
 - Gestionar comunicaciones derivadas del uso de formularios electrónicos.
 - Dar respuesta a peticiones relacionadas con los servicios ofrecidos por la empresa.
- b) Gestión comercial y precontractual.
 - Formalizar la inscripción o registro del usuario como posible cliente.
 - Desarrollar actividades propias de la etapa precontractual.
 - Realizar seguimiento a oportunidades comerciales generadas a través de canales digitales.
 - Gestionar bases de datos de prospectos comerciales.
- c) Promoción, publicidad y marketing digital.
 - Realizar actos de promoción y publicidad de los servicios de seguridad Dissel Ltda.
 - Enviar información comercial, institucional o promocional.
 - Difundir contenidos de interés relacionados con el portafolio de servicios.
 - Ejecutar campañas de marketing digital, email marketing y posicionamiento de marca.
- d) Análisis estadístico y mejora de la experiencia digital.
 - Analizar hábitos de navegación y uso de la página web.
 - Elaborar estadísticas internas y estudios de comportamiento digital.
 - Mejorar la funcionalidad, seguridad y experiencia del usuario en los portales web.
 - Optimizar contenidos, servicios y estrategias digitales.
- e) Gestión tecnológica y seguridad de la información.
 - Administrar la seguridad de los sistemas de información y plataformas digitales.
 - Prevenir fraudes, accesos no autorizados o usos indebidos de los portales.
 - Detectar y mitigar incidentes de seguridad informática.
 - Realizar auditorías, monitoreo y controles de acceso lógico.
- f) Cumplimiento legal y atención de autoridades.
 - Cumplir obligaciones legales, regulatorias y contractuales.

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

- Atender requerimientos de autoridades administrativas, judiciales o de control.
- Conservar evidencias digitales cuando sea requerido legalmente.
- Realizar transmisión y/o transferencia de datos a proveedores tecnológicos, aliados estratégicos o encargados del tratamiento, cuando sea necesario para el funcionamiento de la página web y la prestación de servicios digitales, garantizando el cumplimiento de los estándares legales de protección de datos.

8.2. Conservación de la información

Los datos personales de los visitantes y usuarios de la página web serán conservados por un término de seis (6) meses, contados a partir de su recolección o de la última interacción del usuario, y por el tiempo adicional que resulte necesario para cumplir obligaciones legales, contractuales, probatorias o regulatorias.

8.3. Medidas de seguridad

Seguridad Dissel Ltda. implementa medidas técnicas, humanas y administrativas razonables para proteger los datos personales recolectados a través de su página web, incluyendo controles de acceso, protocolos de seguridad informática, cifrado, monitoreo de sistemas y políticas internas de manejo de la información.

9. Clientes

Seguridad Dissel Ltda., en desarrollo de su objeto social y en cumplimiento de las disposiciones constitucionales y legales que regulan la protección de datos personales en Colombia, establece el presente segmento en su Política de tratamiento de datos con el fin de regular el tratamiento de los datos personales de sus clientes, tanto personas naturales como personas jurídicas, incluidos los representantes legales, personas de contrato, funcionarios autorizados, subcontratistas vinculados al cliente y demás terceros relacionados con la relación comercial.


El tratamiento de la información se realizará bajo los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad garantizando en todo momento los derechos de los titulares y la adopción de medidas técnicas, humanas y administrativas razonables para proteger la información contra pérdida, uso indebido, acceso no autorizado o fraudulento.

9.1. Ámbito de aplicación

Aplica para todos los clientes actuales, anteriores y futuros de Seguridad Dissel Ltda., así como:

- Clientes personas naturales.
- Representantes legales de clientes personas jurídicas.
- Funcionarios, empleados o colaboradores designados por los clientes como personas de contacto administrativo, operativo, financiero o contractual.
- Subcontratistas, proveedores o terceros vinculados al cliente cuando su información sea necesaria para la ejecución del contrato.
- Usuarios autorizados dentro de la cadena de manejo de decisiones operativas del cliente.

El tratamiento podrá realizarse de manera manual o automatizada, a través de bases de datos físicas o digitales, sistemas de información, plataformas digitales, sistemas de información, plataformas tecnológicas, aplicaciones corporativas, canales de

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

comunicación, sistemas de grabación y demás mecanismos legítimos utilizados por la organización.

9.2. Recolección de datos personales de clientes

Seguridad Dissel Ltda., recolecta datos personales de clientes a través de medios físicos, digitales y electrónicos, tales como:

- Formularios contractuales y precontractuales.
- Cotizaciones, propuestas comerciales y procesos de negociación.
- Contratos, órdenes de servicio y documentos anexos.
- Canales de atención presencial, telefónica y virtual.
- Sistemas de grabación de llamadas y plataformas de videoconferencias.
- Sistemas de control de acceso, validación biométrica y verificación de identidad.
- Bases de datos compartidas legítimamente por el cliente o terceros autorizados.
- Consultas a listas restrictivas, bases de datos públicas o privadas legalmente habilitadas.

9.3. Finalidades del tratamiento de los datos personales del cliente.

El tratamiento de los datos personales de los clientes se realizará, de manera enunciativa y no limitativa, para las siguientes finalidades generales y específicas.

a. Gestión de la relación comercial y contractual

- Permitir la ejecución, desarrollo y terminación de la relación comercial y contractual entre Seguridad Dissel Ltda., y el cliente.
- Administrar integralmente las etapas precontractuales, contractual y Poscontractual, incluyendo negociaciones, renovaciones, modificaciones y liquidaciones.
- Gestionar el cumplimiento de las obligaciones contractuales adquiridas por las partes.

b. Ejecución del objeto social


- Prestar de manera adecuada los servicios de seguridad, vigilancia, alarmas de seguridad, portería electrónica y vigilancia digital.
- Coordinar operaciones, rutas, procedimientos de seguridad y protocolos definidos con el cliente.
- Gestionar situaciones de riesgos, contingencias, novedades operativas o emergencias asociadas al servicio.

c. Gestión administrativa, contable y financiera

- Realizar procesos de facturación, recaudo, cobro y gestión de cartera, directamente o a través de terceros autorizados.
- Llevar los registros contables, financieros y tributarios exigidos por la ley.
- Realizar análisis financieros, estudios de crédito y evaluaciones de riesgo comercial.
- Reportar, actualizar y consultar información ante centrales de riesgo y operadores de bancos de datos, conforme a la normativa aplicable.

d. Cumplimiento legal y regulatorio

- Cumplir obligaciones legales, contractuales y regulatorias aplicables a la actividad de la empresa.
- Atender requerimientos de autoridades judiciales, administrativas o de control.
- Suministrar información a entidades públicas o privadas cuando exista obligación legal o requerimiento expreso.

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

- Dar cumplimiento a disposiciones relacionadas con prevención de lavado de activos y financiación al terrorismo – LAFT.

e. Gestión de seguridad y control

- Verificar la identidad del cliente y de las personas autorizadas.
- Consultar y validar información en listas de control nacionales e internacionales.
- Administrar sistemas de control de acceso, registro de ingreso y salida y validaciones biométricas.
- Registrar evidencias operativas, grabaciones de llamadas, imágenes y videos relacionados con la prestación del servicio.

f. Tratamiento de datos sensibles

Tratar datos biométricos como huella, voz e imagen para:

- Acreditar consentimiento y autenticación en procesos contractuales.
- Verificar identidad y control de accesos.
- Evaluar la calidad del servicio.
- Registrar reuniones virtuales, capacitaciones, eventos o auditorías.
- Garantizar medidas reforzadas de seguridad y confidencialidad para este tipo de información.

g. Atención al cliente y postventa

- Atender solicitudes, quejas, reclamos y requerimientos.
- Gestionar garantías y servicios posteriores a la contratación.
- Mantener canales de comunicación eficientes con el cliente.

h. Marketing, publicidad y fidelización

- Enviar información comercial, promociones, ofertas y portafolio de servicios.
- Realizar campañas de fidelización y estudios de mercado.
- Invitar a eventos, capacitaciones y actividades institucionales.
- Analizar tendencias del mercado y evaluar la calidad de los servicios.

i. Gestión tecnológica y mejora continua


- Desarrollar proyectos de automatización y transformación digital.
- Implementar mejoras en proceso, productos y servicios.
- Realizar análisis estadísticos y estudios internos.
- Realizar transmisión y/o transferencia de datos personales a terceros, aliados estratégicos o empresas vinculadas, conforme a la política y a los contratos correspondientes.

La información recolectada de clientes corresponde principalmente a: (i) Datos de identificación. (ii) Datos de contacto y ubicación. (iii) Información financiera, comercial y tributaria. (iv) Datos laborales y de representación legal. (v) Datos relacionados con intereses comerciales. (vi) Datos sensibles estrictamente necesarios para las finalidades descritas.

9.4. Conservación de la información

Los datos personales de los clientes serán conservados durante el tiempo en que se mantenga vigente la relación comercial o contractual y, posteriormente, por un término adicional de cinco (5) años, o el que resulte necesario para cumplir las obligaciones legales, contractuales, probatorias o regulatorias.

10. Tratamiento de datos de candidatos, trabajadores y extrabajadores en las diferentes etapas de selección y contractuales.

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

10.1. Objeto del segmento

SEGURIDAD DISSEL LTDA. trata los datos personales y sensibles de los candidatos, trabajadores y extrabajadores en las diferentes etapas de selección, contratación y Poscontractual, garantizando el principio de legalidad, confidencialidad, seguridad, acceso restringido, veracidad y finalidad en el uso de datos personales y sensibles; extiende el tratamiento de los datos en el presente segmento sobre la base de datos, almacenamiento, uso, finalidades y tratamiento.

10.2. Alcance

Aplica a toda la información personal y sensible recolectada, almacenada, usada, circulada, transmitida o suprimida de los candidatos, trabajadores y extrabajadores que intervienen en los procesos de reclutamiento, selección, evaluación, desempeño, retiro y archivo histórico de la empresa.


10.3. Etapas del tratamiento de datos

Etapas de búsqueda de candidatos: En esta etapa, SEGURIDAD DISSEL LTDA, recolecta y trata los datos personales de los candidatos y postulantes que presentan sus hojas de vida o se postulan a vacantes laborales a través de canales como: Plataformas de empleo externas (página web de la empresa, SENA, Confamiliar, portales de empleo, universidades, redes sociales, bolsa de empleo digitales), recepción directa en físico o por correo electrónico institucional, canales internos de comunicación y grupos de difusión autorizados por la empresa; para ello se tienen como formatos asociados al proceso el FO-GH-03 solicitud de aprobación de personal y FO-GH-33 matriz de cargos, educación, formación, habilidades y competencias.

Etapas de preselección y selección: En esta etapa se valoran las competencias, habilidades, actitudes, conocimientos y confiabilidad del candidato para el cargo a desempeñar, para ello se tratan datos como: Información contenida en la hoja de vida, certificados laborales, académicos, resultados de pruebas psicotécnicas, de confiabilidad y conocimiento, referencias personales y laborales verificadas; para ello se tienen como formatos asociados FOR-GH-01 Autorización para el tratamiento de datos personales e información sensible, FO-GH-04 Entrevista de selección, FO-GH-05 Entrevista jefe y/o responsable de área, FO-GH-06 Estudio socioeconómico y/o visita domiciliaria, FO-GH-07 Verificación de referencias laborales y personales, FO-GH-31 Matriz de criticidad de cargos, FO-GH-35 Pruebas de conocimiento.

Etapas precontractual – examen pre ocupacional: Comprende la verificación de antecedentes judiciales, disciplinarios, fiscales y la realización de valoraciones médicas y psicofísicas, para ello se tratan datos como: Antecedentes judiciales, disciplinarios, fiscales y medidas correctivas, resultados de exámenes médicos ocupacionales (ingreso, consumo de drogas y alcohol, psicofísico para porte de armas) datos biométricos (fotografía, huellas, registro dactilar, atendiendo a que la naturaleza de la empresa es la prestación de servicios de seguridad vigilada por la Superintendencia de Vigilancia y Seguridad Privada; para ello se tiene como formatos asociados FO-GH-08 Autorización evaluación de consumo de drogas y alcohol, FO-GH-34 Profesiograma (requisitos médicos por cargo), FO-GH-09 Verificación de documentos, FO-GH-10 Registro individual de firma y huellas.

Etapas contractual: Una vez seleccionado el candidato como apto en todas las etapas del proceso de selección de SEGURIDAD DISSEL LTDA. formaliza su vinculación laboral mediante la suscripción de contrato de trabajo y demás documentos asociados,

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

de conformidad con lo dispuesto por la normatividad laboral y las disposiciones normativas en seguridad privadas y aquellas materia de la Superintendencia de Vigilancia y Seguridad Privada; durante esta etapa, la empresa recolecta, almacena y trata datos personales y sensibles con el fin de gestionar la relación laboral, garantizar el cumplimiento normativo en materia de seguridad privada, salud ocupacional y seguridad social, así como preservar la seguridad integral de las operaciones, clientes, instalaciones, personas y bienes vigilados conocer los datos personales, biométricos y contractuales y de afiliación a seguridad social; para ello se tienen como formatos asociados: FO-GH-11 Entrega de dotación y EPP, FO-GH-13 Acuerdo de confidencialidad, FO-GH-14 Acta de compromiso de conductores, FO-GH-15 Inducción y reinducción de personal, FO-GH-17 Entrenamiento en el cargo, FO-GH-18 Evaluación del periodo de prueba, FO-GH-44 Matriz de dotación y EPP.

Etapa Poscontractual: Corresponde el período posterior a la terminación del vínculo laboral entre el trabajador y SEGURIDAD DISSEL LTDA., cualquier sea la causa que origine dicha desvinculación (renuncia voluntaria o motivada, terminación del contrato por justa o sin justa causa, finalización del contrato a término fijo o decisión unilateral). Durante esta etapa, la empresa conserva, custodia y trata la información personal, laboral y sensible del extrabajador, únicamente para los fines autorizados por la ley y las políticas internas, garantizando la confidencialidad, integridad y disponibilidad de la información. El tratamiento se ajusta a las obligaciones de conservación documental derivadas del Código Sustantivo de Trabajo, para ello se tratan datos como: Información laboral histórica (hojas de vida, contratos laborales, actas de terminación, evaluaciones de desempeño, sanciones disciplinarias, constancias de inducción y reinducción, registros de capacitación, entrenamientos, entre otras suscritas entre el trabajador y la empresa), información sobre seguridad social (aportes y periodos cotizados a EPS, AFP, ARL, Cajas de compensación, Fondo de Cesantías y demás entidades del Sistema de Seguridad Social), información tributaria y fiscal (ingresos laborales, retenciones practicadas, certificados de ingresos y retenciones, reportes a la DIAN y demás documentos contables y fiscales asociados) datos de seguridad (registros de acceso, reportes de inventarios, devoluciones de elementos de dotación, carnetización, entrega de credenciales, constancia de paz y salvo administrativo, entre otros) y de contacto actualizados; para ello se tienen como formatos asociados: FO-GH-23: Registro paz y salvo de retiro, FO-GH-11: Entrega y devolución de dotación y elementos de protección personal, FO-GH-15 / FO-GH-16 / FO-GH-17: Registros de inducción, reinducción y entrenamiento en el cargo, FO-GH-18: Evaluación final de periodo de prueba (para historial de desempeño), FO-GH-19: Reporte de incidentes o accidentes de trabajo (si existieron durante la relación laboral), Documentos de nómina y certificados tributarios: generados a través del software de gestión humana Venimous o sistemas autorizados equivalentes.

10.4. **Recolección de los datos personales del candidato.**

La empresa SEGURIDAD DISSEL LTDA recolecta la información de los candidatos que presentan sus propuestas a través de los canales facilitados para la búsqueda de ofertas de empleo, así como, los datos recolectados en la etapa de preselección, selección y precontractual.

10.5. **Finalidades del tratamiento de los datos personales del candidato.**

El almacenamiento, circulación, tratamiento y supresión de datos de la empresa de los candidatos tendrá para las finalidades expuestas para cada etapa, las cuales se



SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST

COD: OD-DE-10

POLÍTICA TRATAMIENTO DE DATOS

VERSION: 1

encuentran alineados a la normatividad respecto al tratamiento de datos, ley 1581 de 2012 y decreto 1377 de 2013.

Titular del derecho-candidatos	Finalidad
Etapa de búsqueda de candidatos	<ul style="list-style-type: none"> ● Recolectar, registrar y analizar los datos del candidato para verificar que cumpla con los requisitos mínimos del cargo ofertado. ● Contactar al candidato por medios electrónicos o telefónicos para coordinar entrevistas o pruebas de selección. ● Administrar los procesos de reclutamiento, almacenamiento y clasificación de hojas de vida. ● Conservar los datos de los candidatos no seleccionados, previo consentimiento, para futuras oportunidades laborales a fines. ● La empresa recolecta los datos del candidato como nombre, cédula, formación académica, experiencia laboral, información que se ajuste a los requisitos mínimos expuestos en la oferta laboral, y así, poder evaluar el primer filtro. ● Contacto a través de llamada, mensaje de datos WhatsApp y/o correo electrónico para la comunicación con el candidato que cumple con las condiciones mínimas, informando sobre el proceso de selección, entrevista y recepción de documentos. ● Con el consentimiento del candidato se conservan los datos para futuras ofertas laborales que se ajusten al perfil, se almacena la información. ● Con la información de las ofertas la empresa organiza y administra el proceso de selección, incluyendo la programación de entrevistas, la evaluación de los candidatos y la toma de decisiones para la etapa de preselección y selección. ● La empresa trata los datos para cumplir con el proceso de búsqueda de candidatos para las ofertas laborales.
	<ul style="list-style-type: none"> ● Evaluar las competencias, conocimientos, habilidades y rasgos psicológicos del candidato frente al perfil del cargo.




SISTEMA INTEGRADO DE GESTION
CALIDAD-CONTROL Y SEGURIDAD-SST

COD: OD-DE-10

POLÍTICA TRATAMIENTO DE DATOS

VERSION: 1

<p>Etapa de preselección y selección.</p>	<ul style="list-style-type: none">● Realizar estudios socioeconómicos y/o visitas domiciliarias para validar la información aportada y verificar condiciones de entorno y seguridad.● Validar referencias laborales, académicas y personales para garantizar la idoneidad e integridad del candidato.● Determinar la elegibilidad del candidato en el proceso de selección y documentar el resultado del proceso.● Realizar pruebas psicotécnicas y de confiabilidad conforme al perfil de riesgo del cargo, especialmente en cargos críticos.● La empresa recolecta los datos del candidato, y solicita la documentación para realizar la validación de los datos mencionados por el candidato, a través de la revisión de la hoja de vida, certificados académicos, referencias y certificados laborales, así como, demás documentación profesional requerida para el cargo.● Se realizan pruebas escritas y/o verbales para la evaluación del candidato para el proceso de selección, esta información queda recopilada y es tratada para los fines de la selección, conocer las habilidades, aptitudes, actitudes y conocimiento del cargo del candidato y evaluarlas.● Llamadas telefónicas y entrevistas con el área de Gestión Humana y con el líder del área al que está ofertando el candidato.● La información recopilada será destinada para llevar a cabo el proceso de preselección y selección del candidato.
<p>Etapa precontractual</p>	<ul style="list-style-type: none">● Validar los antecedentes judiciales, disciplinarios y fiscales del candidato, garantizando la transparencia y confiabilidad del proceso.● Cumplir con los requisitos de la Superintendencia de Vigilancia y Seguridad Privada para la idoneidad del personal que porte o manipule armas.● Determinar la aptitud física, mental y emocional del candidato para desempeñar el cargo con seguridad.● Evaluar el riesgo psicosocial y prevenir afectaciones a la seguridad propia y de terceros.

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1


	<ul style="list-style-type: none"> ● Documentar y conservar los resultados de las pruebas médicas, psicofísicas y de consumo de sustancias conforme al cargo. ● La verificación de antecedentes permite a la empresa cumplir con la política de transparencia y facilitar un entorno libre de riesgos para los integrantes directos e indirectos de la empresa, además, que la empresa tiene un área destinada a la exportación y negocios internacionales, por lo que, la normatividad recomienda estas prácticas. ● La verificación de los exámenes ocupacionales le permite a la empresa evaluar la condición física y mental del candidato para poder desempeñar la función y cargo ofertado de manera segura para su integridad, la de sus compañeros y la productividad de la empresa. ● La demás información recopilada se realizará con la finalidad de culminar y evaluar la etapa contractual y serán tratados para tales fines.
--	--

10.6. De la base de datos de trabajadores

La empresa SEGURIDAD DISSEL recolecta la información de los trabajadores, así como su documentación para el cumplimiento de las exigencias normativas estipuladas en el Código Sustantivo de Trabajo, disposiciones de la Superintendencia de Vigilancia y Seguridad Privada y demás normas concordantes.

10.7. Finalidades del tratamiento de los datos personales de trabajadores.


Titular del derecho trabajador	Finalidad
	<ul style="list-style-type: none"> ● Gestionar la relación laboral conforme al contrato y a la normatividad vigente. ● Cumplir con las obligaciones legales en materia laboral, de seguridad social y parafiscales. ● Administrar los registros de asistencia, desempeño, sanciones disciplinarias y demás evidencias de la relación laboral. ● Garantizar la seguridad de los trabajadores mediante la implementación del SG-SST y las políticas de videovigilancia.

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

<p>Etapa contractual</p>	<ul style="list-style-type: none"> ● Controlar el acceso físico y digital del personal operativo mediante datos biométricos y credenciales emitidas por la Superintendencia de Vigilancia y Seguridad Privada. ● Para el cumplimiento de las obligaciones legales la empresa trata, compila y almacena los documentos como contrato laboral, acuerdo de confidencialidad y autorización de tratamiento de datos al momento de la vinculación laboral a la empresa. ● Para el cumplimiento de las obligaciones de pensiones y parafiscales, así como, seguridad social, la empresa solicita información como certificado de salud y pensiones, y lo inscribe a ARL solicitando información para tales fines. ● La empresa solicita los datos personales para la gestión y administración del Recurso humano, así como, facilitar la información interna. ● Para velar el cumplimiento de las políticas internas, Reglamento Interno de Trabajo, Contrato Individual de Trabajo, Sistema de Gestión de Seguridad y Salud en el Trabajo, así como, así como realizar las sanciones disciplinarias, documentar la diligencia de descargos, llamados de atención, actas de compromiso, suspensiones, actas de finalización, actas de terminación del contrato por justa causa y sin justa causa, pago de salarios y prestaciones sociales, preavisos, se almacena, compila y trata la información documental del trabajador. ● Cumplir con las disposiciones de la resolución 0312 de 2019 sobre el Sistema de Gestión de Seguridad y Salud en el Trabajo. ● Velar por la seguridad de los trabajadores y demás estipulaciones redactas en la política de videovigilancia sobre el tratamiento de datos biométricos, personales y sensibles. ● La demás información recopilada será con la finalidad de dar cumplimiento de las diferentes obligaciones normativas colombianas e internacionales.
--------------------------	--

10.8. De la base de datos de los extrabajadores

La empresa SEGURIDAD DISSEL LTDA almacena y custodia la información de los extrabajadores para cumplir con las obligaciones normativas de Colombia y el adecuado tratamiento de datos consignado en la ley 1581 de 2012, además de poder facilitar la información solicitada por las entidades y autoridades competentes.

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1


10.9. Finalidades del tratamiento de los datos personales de extrabajadores.

Titular del derecho extrabajador	Finalidad
Etapa Poscontractual	<ul style="list-style-type: none"> ● Cumplir con las obligaciones legales y laborales posteriores al retiro. ● Atender solicitudes y requerimientos de entidades públicas y privadas. ● Suministrar información histórica laboral y de seguridad social al extrabajador o a las autoridades competentes. ● Conservar evidencia documental de la relación laboral en cumplimiento de la normatividad laboral. ● Cumplir con las obligaciones fiscales y tributarias ● Garantizar la trazabilidad en materia de seguridad y control operativo, especialmente en cargos que implicaron el porte de armas, custodia de bienes o manejo de información sensible, manteniendo registro de dotación y credenciales hasta la confirmación de su devolución. ● Facilitar procesos de referencia laboral, exclusivamente previa autorización expresa del extrabajador o requerimiento legal, asegurando que la información emitida sea veraz, pertinente y proporcional. ● Realizar actualizaciones o verificaciones de contacto. ● Almacenar los expedientes laborales físicos y laborales bajo custodia del área de Gestión Humana y/o del responsable del cumplimiento, con protocolos de seguridad que garanticen la protección de la información sensible y confidencial.

10.10. . Tratamiento de datos sensibles

En desarrollo de las etapas de selección, contratación y permanencia laboral, SEGURIDAD DISSEL LTDA. realiza el tratamiento de datos sensibles de candidatos, trabajadores y extrabajadores, conforme a lo dispuesto por la Ley 1581 de 2012, el Decreto 1377 de 2013, la Circular Externa 003 de 2018 de la SIC y la Resolución 0312 de 2019 (SG-SST).


Datos sensibles tratados

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

1. Resultados de pruebas de consumo de drogas y alcohol (FO-GH-08): Se realizan como parte del proceso de selección o durante la relación laboral, especialmente para personal clasificado como crítico o con responsabilidades de porte y manejo de armas. Estas pruebas permiten verificar el cumplimiento de las normas de confiabilidad y sobriedad exigidas por la Superintendencia de Vigilancia y Seguridad Privada, así como prevenir incidentes que pongan en riesgo la vida, la integridad o los bienes custodiados.
2. Valoraciones médicas ocupacionales y psicofísicas (FO-GH-34): Incluyen los exámenes médicos de ingreso, periódicos, de retiro, de seguimiento y psicofísicos exigidos para personal operativo (guardas, supervisores, jefes de operaciones, técnicos de medios tecnológicos y demás cargos críticos). Su objetivo es verificar la aptitud médica, psicológica y física del trabajador para desempeñar funciones de seguridad armada, conducción, manipulación de equipos eléctricos o vigilancia con medios tecnológicos, conforme al profesiograma de la empresa.
3. Huellas dactilares, fotografías y registros biométricos (FO-GH-10): Se capturan en el registro individual de firma y huellas, carnetización y control de ingreso y salida a instalaciones o turnos de servicio. Estos datos son tratados para garantizar la autenticación, la trazabilidad del personal, el control de acceso físico y digital, y la prevención de fraudes o suplantaciones de identidad.
4. Información sobre condiciones de salud y restricciones médicas (FO-GH-02, FO-GH-20, FO-GH-21): Comprende el autorreporte de condiciones de salud, recomendaciones médicas ocupacionales y perfil sociodemográfico del trabajador, utilizados en el marco del Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST) para adaptar medidas preventivas, identificar riesgos laborales y garantizar ambientes de trabajo seguros y saludables.

Finalidades específicas del tratamiento de datos sensibles

1. Cumplir con los requisitos de idoneidad, confiabilidad y aptitud exigidos por la Supervigilancia para el personal de seguridad privada, incluyendo la evaluación psicofísica y de consumo de sustancias, asegurando la competencia y estabilidad emocional del personal operativo y de supervisión.
2. Determinar la aptitud médica, psicológica y física de los trabajadores para desempeñar funciones críticas o de alto riesgo (porte de armas, instalación de alarmas, operación de sistemas eléctricos o tecnológicos).
3. Garantizar la seguridad física y electrónica de las instalaciones, trabajadores, clientes y usuarios, mediante el uso de tecnologías de videovigilancia, control biométrico y sistemas de acceso, conforme a la Ley 1928 de 2018 y a las políticas internas de seguridad tecnológica.
4. Aplicar medidas de prevención, apoyo o restricción derivadas de las valoraciones de salud ocupacional y de las recomendaciones médicas, conforme a lo dispuesto en la Resolución 0312 de 2019, la Ley 1616 de 2013 (salud mental laboral) y las políticas del SG-SST.
5. Controlar el cumplimiento del reglamento interno de trabajo, las políticas de ética y conducta, las pruebas de confiabilidad y los protocolos de prevención de

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

riesgos, garantizando un entorno seguro y libre de consumo de sustancias psicoactivas.

- Cumplir con las obligaciones contractuales, disciplinarias y legales frente a entidades públicas y privadas (Ministerio del Trabajo, ARL, EPS, AFP, UGPP, Fiscalía General de la Nación o Supervigilancia), mediante la entrega o conservación de registros requeridos.

10.12. Almacenamiento y conservación

Toda la información recolectada en los procesos de selección, contratación, permanencia y retiro del personal se conserva bajo estrictos criterios de **seguridad, integridad y confidencialidad**, en los siguientes medios y condiciones:

Medios de almacenamiento

- Carpeta física individual:** Contiene toda la documentación precontractual, contractual y poscontractual (hojas de vida, certificados, exámenes, actas, contratos, registros de inducción, sanciones, etc.). Estas carpetas son custodiadas exclusivamente por el área de Gestión Humana en archivo físico con acceso restringido a personal autorizado.
- Carpeta digital institucional:** Cada trabajador y candidato cuenta con un expediente digital almacenado en la nube institucional o servidor interno bajo protocolos de cifrado o contraseña. Se gestiona mediante el software Venimous u otras plataformas seguras de gestión humana que garantizan la trazabilidad y auditoría de accesos.
- Bases de datos seguras:** Los registros de control de acceso, videovigilancia, biometría y evaluación médica se integran en sistemas protegidos con estándares de seguridad ISO 27001 y políticas de respaldo, actualización y recuperación de información ante incidentes.


Plazo de conservación

- Mínimo 10 años contados a partir de la terminación de la relación laboral, en cumplimiento de las normas laborales y tributarias (art. 632 del Estatuto Tributario y art. 264 del CST).
- Hasta 20 años o de forma indefinida para datos relacionados con cargos armados, investigaciones judiciales, hechos de seguridad o procesos disciplinarios, según las disposiciones de la Supervigilancia.
- La información de candidatos no vinculados se conservará **por un periodo máximo de 2 años**, con fines de posibles futuras convocatorias, previa autorización del titular.

10.13. Seguridad de la información

SEGURIDAD DISSEL LTDA. adopta medidas técnicas, humanas y administrativas orientadas a proteger los datos personales y sensibles de accesos no autorizados, pérdida, alteración o uso indebido, de acuerdo con los principios de seguridad y confidencialidad consagrados en la Ley 1581 de 2012 y en las mejores prácticas internacionales de gestión de información.

Medidas técnicas

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

- Implementación de sistemas de autenticación mediante usuario y contraseña individual.
- Control de acceso biométrico y videovigilancia en las áreas de archivo y almacenamiento.
- Cifrado de bases de datos y respaldo automatizado en la nube institucional.
- Protección de la red interna mediante firewall y antivirus de seguridad corporativa.
- Eliminación segura de archivos digitales y físicos conforme a la política de retención documental.

Medidas humanas y administrativas

- Suscripción de acuerdos de confidencialidad (FO-GH-13) con todo el personal que tenga acceso a información sensible.
- Capacitaciones periódicas en protección de datos, seguridad de la información y manejo ético de información sensible, especialmente dirigidas al personal operativo y de gestión humana.
- Restricción de accesos por niveles de responsabilidad y función.
- Protocolos de custodia, traslado y eliminación segura de documentación física.
- Auditorías internas periódicas sobre cumplimiento de la política de tratamiento de datos personales.

Responsabilidad y control

El área de Gestión Humana actúa como responsable del tratamiento en este segmento, y el Oficial de cumplimiento supervisa el cumplimiento de las medidas técnicas y normativas.

Cualquier incidente de seguridad será reportado de inmediato a la Superintendencia de Industria y Comercio (SIC) conforme al procedimiento de notificación de vulneraciones de datos personales.


11. Tratamiento de datos de familiares y beneficiarios de los trabajadores.

De conformidad con lo dispuesto en el artículo 10 de la ley 1581 de 2012, Seguridad Dissel Ltda., informa que no será necesaria la autorización previa, expresa e informado del titular para el tratamiento de los datos personales de los familiares y beneficiarios de los trabajadores, cuando dicho tratamiento resulte necesario para el cumplimiento de obligaciones legales y laborales a cargo del empleador, o se encuentre amparado por alguna de las excepciones previstas en la ley.

Este tratamiento se realizará para las finalidades legítimas, necesarias y proporcionales, derivadas de la relación laboral existente con el trabajador titular principal de la información.

11.1. Ámbito de aplicación

Los datos personales de familiares y beneficiarios de los trabajadores vinculados a Seguridad Dissel Ltda., cuya información sea suministrada por el trabajador o requerida por la empresa para el cumplimiento de obligaciones laborales y legales, de seguridad social, bienestar y atención de emergencias.

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

El tratamiento de los datos se efectuará en el marco del desarrollo del objeto social de la empresa, el cumplimiento normativo legal, especialmente el laboral y de seguridad social vigente, y la atención a requerimientos de autoridades competentes.

11.2. Recolección de datos personales de familiares y beneficiarios

Seguridad Dissel Ltda., podrá recolectar y tratar datos personales de familiares y beneficiarios de los trabajadores sin requerir autorización directa del titular, cuando dicho tratamiento sea necesario para: (i) Cumplir obligaciones legales a cargo del empleador establecidas en la legislación laboral, de seguridad social y normas concordantes. (ii) Atender requerimientos de entidades administradoras del sistema de seguridad social, cajas de compensación familiar u otras autoridades competentes. (iii) Gestionar situaciones de urgencia médica o sanitaria. (iv) Administrar registros exigidos por la ley derivados de la relación laboral.

La recolección de los datos se realizará a través de medios físicos y digitales, formularios internos de sistemas de información, soportes documentales, software, plataforma interna de la empresa, y demás mecanismos legítimos.

11.3. Finalidades del tratamiento de los datos personales

El tratamiento de los datos personales de los familiares y beneficiarios de los trabajadores se realizará, entre otras, para las siguientes finalidades:

- Cumplir las obligaciones legales y laborales a cargo del empleador, determinadas por la legislación laboral colombiana o impartidas por autoridades administrativas o judiciales.
- Gestionar la afiliación, actualización y administración de los beneficiarios del trabajo en el sistema de seguridad social integral y en las cajas de compensación familiar.
- Realizar, documentar y conservar soportes relacionados con programas de bienestar, actividades recreativas, culturales o de integración derivados de la relación laboral.
- Efectuar notificaciones y contactos en situaciones de emergencia, accidentes laborales o eventos que afecten la integridad del trabajador.
- Administrar y conservar los registros exigidos por la normatividad laboral y de seguridad social durante el tiempo legalmente establecido.

Tratamiento de datos de contratistas y proveedores de la empresa SEGURIDAD DISSEL LTDA.


10. De los datos personales de los contratistas vinculados

En el desarrollo de sus actividades, SEGURIDAD DISSEL LTDA, en cumplimiento de la normatividad vigente sobre protección de datos, realiza el tratamiento de la información de sus contratistas y proveedores, sean personas naturales o jurídicas, conforme a las finalidades, tratamiento y almacenamiento.

11.1. Definiciones

Contratistas: Persona natural o jurídica que se vincula con una entidad contratante mediante la celebración de un contrato, cuya obligación es cumplir y ejecutar el objeto de este, el cual puede constituir en bienes, obras o servicios.

(Agencia Nacional de Seguridad Vial).

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

Proveedor: Persona natural o jurídica que provee bienes, insumos o servicios a un cliente, entidad o persona con fines de lucro; quien ofrece, suministra, distribuye y comercializa un producto.

11.2. Recolección de los datos personales de Contratistas como persona natural y jurídica

SEGURIDAD DISSEL LTDA recolecta la información de sus contratistas y proveedores mediante los formularios de registro, hojas de vida, propuestas, certificaciones, documentos de identidad, certificados de existencia y representación legal, RUT, certificados bancarios, comprobantes de pago de aportes de seguridad social, antecedentes judiciales, fiscales y disciplinarios, licencias o permisos de funcionamiento, y demás documentos necesarios para la evaluación, vinculación y control de la relación contractual o comercial.

Asimismo, podrá recolectar datos biométricos, videograbaciones o registros de acceso cuando el contratista o proveedor ingrese a las instalaciones o interactúe con los sistemas de videovigilancia, portería electrónica y monitoreo de alarmas de la empresa.

11.3. Finalidades del tratamiento de los datos personales de contratistas como persona natural y jurídica.

El almacenamiento, circulación y tratamiento de datos en la empresa de los contratistas como persona natural y jurídica tendrán las finalidades para cada caso, las cuales se encuentran alineados a la normatividad respecto al tratamiento de datos ley 1581 de 2012 y decreto 1377 de 2013.

Titular del derecho	Finalidad
Contratista – persona natural – Civil y/o comercial	<ul style="list-style-type: none"> ● Exigir la cotización a ARL para el desplazamiento dentro de las instalaciones físicas de la empresa, almacenamiento de información de soportes de pago de seguridad social como independiente. ● Tratar los datos personales como nombre completo, cédula, número de teléfono y correo electrónico para la comunicación y ejecución del contrato. ● Evaluar la tapa precontractual para la evaluación de las competencias y alcances para la prestación del servicio como hoja de vida, diplomas, certificados, referencias del servicio. ● Evaluar la tapa contractual, número de cuenta bancaria y certificado de pago de seguridad social en salud, pensiones y ARL, cumpliendo con las obligaciones normativas colombianas respecto a seguridad social y parafiscales, así como, el desembolso de los honorarios a la cuenta bancaria. ● Cumplir con las obligaciones fiscales, tributarias como declaración de renta, retenciones de fuente, aportes a la seguridad social. ● Prevenir riesgos laborales, información sobre condiciones de salud del contratista para la mitigación del riesgo.




SISTEMA INTEGRADO DE GESTION
CALIDAD-CONTROL Y SEGURIDAD-SST

COD: OD-DE-10

POLÍTICA TRATAMIENTO DE DATOS

VERSION: 1

	<ul style="list-style-type: none">● Garantizar el control de ingreso a instalaciones, áreas críticas o zonas de monitoreo mediante sistemas de videovigilancia.● Monitorear las actividades sospechosas, sistemas de información, verificación de identidad, registro de incidentes y/o accidentes.● Cumplir las obligaciones legales fiscales, penales y contractuales.● Expedir los antecedentes fiscales, procuraduría, legales, búsqueda de procesos civiles en la rama judicial, certificado de medidas restrictivas, policía nacional, antecedentes contraloría con fines a la protección y seguridad de la empresa.
<p>Contratista – Persona jurídica – Jurídica - Civil y/o comercial.</p>	<ul style="list-style-type: none">● Identificar la razón social, NIT, dirección de domicilio legal, número de contacto y correo electrónico, identificación del contratista.● Evaluar la capacidad financiera, técnica y de cumplimiento, a través de la revisión de estados financieros, certificados de existencia y representación legal, y referencias comerciales.● Gestionar el pago de honorarios o contraprestaciones mediante la validación de información bancaria y fiscal.● Conocer información como RUT, declaraciones de renta, retenciones de fuente, certificado de pagos de parafiscales y aportes de seguridad social para el cumplimiento de las obligaciones legales y fiscales.● Convocar a reuniones, envío de correo electrónicos, cualquier comunicación para el desarrollo del contrato, monitorio de sistema de videovigilancia comunicaciones internas y control de acceso de instalaciones.● Verificar la identidad, control de acceso, monitoreo de actividades sospechosas, análisis de causas, medidas para la seguridad de información.● Declarar la información exógena, retenciones de impuestos y retenciones de impuestos de renta y retenciones de IVA, afiliación de trabajadores para el cumplimiento de las obligaciones legales.● Expedir los antecedentes fiscales, procuraduría, legales, búsqueda de procesos civiles en la rama judicial, certificado de medidas restrictivas, policía nacional, antecedentes contraloría con fines a la protección y seguridad de la empresa.● Cumplir con la normativa sectorial expedida por la Superintendencia de Vigilancia y Seguridad Privada especialmente en materia de control de idoneidad y antecedentes.● Atender solicitudes de información de entidades públicas o de control.

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

12. De la base de datos de proveedores

SEGURIDAD DISSEL LTDA recolecta información de sus proveedores con fines de gestión administrativa, contable, logística, comercial y de control de calidad, así como para la adquisición de bienes, materiales, tecnología y servicios vinculados con las operaciones de vigilancia privada, videovigilancia y monitoreo.


12.1. Finalidades del tratamiento de los datos personales de contratistas como persona natural y jurídica.

Titular del derecho	Finalidad
Proveedor – persona natural y jurídica	<ul style="list-style-type: none"> ● Identificar y registrar datos básicos de identificación del proveedor (nombre, NIT, contacto, dirección, correo electrónico). ● Gestionar pagos, facturación, créditos y obligaciones contractuales, verificando la información bancaria y contable. ● Cumplir con las obligaciones fiscales y tributarias: declaraciones de renta, retenciones, aportes a seguridad social y reportes de información exógena. ● Expedir antecedentes fiscales, procuraduría, legales, búsqueda de consulta de procesos en rama judicial, certificado de medidas restrictivas, policía nacional, antecedentes de contraloría y los demás con fines a la protección y seguridad de la empresa. ● Garantizar la trazabilidad, seguridad y conformidad de los equipos o sistemas adquiridos conforme a la normatividad técnica y de protección de datos. ● Informar sobre los bienes, insumos, como sus características, precios, datos comerciales, financieros respecto al suministro y demás intrínsecos en la relación comercial, proveedor – cliente. ● Comunicar el envío de correos y todas aquellas comunicaciones respecto al suministro, venta, compra, reclamaciones, entre otras de los bienes y/o servicios. ● Cumplir con requerimientos de autoridades judiciales o administrativas.

12.2. Almacenamiento

La información recolectada de contratistas y proveedores será almacenada en medios físicos y digitales seguros (archivos, bases de datos, servidores o nube), bajo medidas técnicas, humanas y administrativas adecuadas para prevenir pérdida, acceso no autorizado o tratamiento indebido.

En algunos casos, la empresa podrá delegar la custodia documental a terceros mediante contratos de confidencialidad y protección de datos.

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

La conservación de los datos se efectuará durante el término necesario para cumplir las finalidades señaladas o mientras exista obligación legal o contractual que lo justifique.

13. Transmisión y transferencia nacional e internacional de datos.

13.1. Ámbito de aplicación

Aplica la transmisión y transferencia de datos personales de trabajadores, extrabajadores, contratistas, proveedores, clientes, potenciales clientes, accionistas y demás titulares cuyos datos personales sean tratados por Seguridad Dissel Ltda., ya sea en calidad de responsable del tratamiento o, cuando corresponda, en calidad de Encargado del tratamiento. La transmisión o transferencia podrá realizarse a terceros ubicados dentro o fuera del territorio nacional, siempre que exista una finalidad legítima, se adoptan las medidas de seguridad exigidas por la ley y se garantice la protección adecuada de los datos personales.

13.2. Definiciones

Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos a un tercero, dentro o fuera del territorio nacional, que actúa como Encargado del tratamiento, en nombre y por cuenta de la empresa.

Transferencia: Tratamiento de datos personales que implica el envío de información a un tercero, dentro o fuera del territorio nacional, que actúa como responsable del Tratamiento y decide sobre la finalidad y uso de los datos.

Encargado de tratamiento de datos: Persona natural o jurídica que realiza el tratamiento de datos personales por cuenta del responsable, conforme a las instrucciones impartidas por este.


13.3. Tratamiento de datos personales en calidad de encargado

En aquellos casos en los que Seguridad Dissel Ltda. actúe como Encargado del Tratamiento, los datos personales serán tratados exclusivamente con base en la relación contractual existente con el cliente, y únicamente para las finalidades necesarias para la prestación del servicio contratado. Dicho tratamiento se realizará durante la vigencia de la relación contractual, garantizando que los datos sean utilizados conforme a las instrucciones del Responsable del tratamiento, sin destinarlos a fines distintos, y adoptando las medidas de seguridad técnicas, humanas y administrativas exigidas por la normatividad vigente.

13.4. Transmisión y transferencia nacional de datos personales

Seguridad Dissel Ltda. podrá transmitir o transferir datos personales a terceros ubicados en el territorio nacional, en los siguientes escenarios generales:

- A autoridades judiciales, administrativos, fiscales o de control, cuando sea requerido en ejercicio de sus funciones legales o por orden expresa de autoridad competente,
- A asesores, consultores, auditores, profesionales y proveedores de servicios legales, contables, financieros, tecnológicos, administrativos, de seguridad, innovación o auditoría, cuando su intervención sea necesaria para el cumplimiento de obligaciones legales, contractuales o corporativas.
- A empresas vinculadas, matrices, subordinadas o pertenecientes a un mismo grupo empresarial, cuando la circulación de la información sea necesaria para la

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

ejecución de procesos administrativos, operativos, de control interno, cumplimiento normativo o gestión corporativo.

- A aliados estratégicos o terceros con los cuales existan acuerdos comerciales vigentes, cuando la transmisión o transferencia sea indispensable para la correcta prestación de los servicios contratados o el desarrollo de actividades conexas o complementarias.

13.5. Transmisión y transferencia internacional de datos personales

Seguridad Dissel Ltda. podrá realizar transmisión o transferencia internacional de datos personales en los siguientes eventos:

- Cuando sea necesario delegar en terceros el almacenamiento, custodia o procesamiento de información en servidores o infraestructuras tecnológicas ubicadas fuera del territorio nacional.
- Cuando, en el marco de su estructura corporativa, sea necesario compartir información con empresas pertenecientes a un grupo empresarial de carácter internacional, para fines administrativos, operativos, de control, cumplimiento o soporte corporativo.

En estos casos, la empresa verificará que el país receptor ofrezca niveles adecuados de protección de datos personales, equivalentes o superiores a los exigidos por la ley 1581 de 2012. Asimismo, se suscribirán los acuerdos de transmisión de datos exigidos por el artículo 25 del Decreto 1377 de 2013, o se obtendrá la autorización del titular cuando esta sea legalmente requerida.

13.6. Medidas de seguridad y obligaciones de terceros

En toda transmisión o transferencia de datos personales, Seguridad Dissel Ltda.


- Exigirá a los terceros la adopción de medidas de seguridad técnicas, humanas y administrativas adecuadas.
- Limitará el acceso a los datos únicamente al personal autorizado y para las finalidades previamente definidas.
- Prohibirá el uso de la información para fines distintos o incompatibles con aquellos que motivaron su recolección.
- Supervisará, cuando sea aplicable, el cumplimiento de las obligaciones contractuales y legales en materia de protección de datos personales.

14. Niños, niñas y adolescentes

En desarrollo de su objeto social y en observancia del marco normativo colombiano sobre protección de datos personales, establece el presente segmento con el fin de regular el tratamiento excepcional de datos personales de niños, niñas y adolescentes, garantizando en todo momento la protección reforzada de sus derechos fundamentales y el respeto por el interés superior del menor.

14.1. Ámbito de aplicación

Este segmento aplica únicamente en aquellos casos excepcionales y necesarios en los que la empresa, pueda llegar a tratar datos personales de niños, niñas y adolescentes, de manera indirecta, principalmente en el marco de relaciones laborales, obligaciones

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

legales del empleador o actividades de bienestar dirigidas a los trabajadores y sus familias.

La empresa no recolecta ni trata de manera directa datos personales de menores de edad como parte de su actividad comercial o de prestación de servicios.

14.2. Principios y marco normativo aplicable

El tratamiento de datos personales de niños, niñas y adolescentes se regirá por lo dispuesto en el artículo 7 de la ley 1581 de 2012, el artículo 44 de la Constitución Política, la ley 1098 de 2006, y los lineamientos impartidos por la SIC – Superintendencia de Industria y Comercio, garantizando de manera prevalente el interés superior del menor y el respeto por sus derechos fundamentales.

14.3. Recolección y tratamiento excepcional

Cuando, de manera excepcional, resulte necesario tratar datos personales de menores de edad, Seguridad Dissel Ltda.:

- Limitará el tratamiento a datos estrictamente necesarios, principalmente de identificación.
- Verificará que la finalidad responda a obligaciones legales o actividades legítimas relacionadas con el bienestar del trabajador y su núcleo familiar.
- Obtendrá la autorización previa, expresa e informada del representante legal o tutor del menor.
- Adoptará medidas técnicas, humanas y administrativas reforzadas para garantizar la confidencialidad y seguridad de la información.

14.4. Finalidad del tratamiento

El tratamiento excepcional de datos personales de niños, niñas y adolescentes tendrá como finalidades generales:

- Cumplir obligaciones legales y laborales a cargo del empleador.
- Gestionar afiliaciones y beneficios derivados del sistema de seguridad social y cajas de compensación.
- Desarrollar actividades de bienestar, recreación o integración familiar dirigidas a los trabajadores.
- Atender situaciones de emergencia que requieran contacto con familiares o beneficiarios del trabajador.


Autorización para el tratamiento de datos personales

14.5. Autorización para el tratamiento de datos personales

Seguridad Dissel Ltda. realizará el tratamiento de datos personales previa autorización expresa, previa e informada del titular, salvo en los casos exceptuados por la ley. La autorización será solicitada por medios físicos, electrónicos o en cualquier formato que garantice su posterior consulta a través de herramientas físicas o técnicas, cumpliendo con los requisitos generales de ley.

Autorización por conductas inequívocas

De conformidad con el artículo 7 del Decreto 1377 de 2013, se entenderá que el titular ha otorgado autorización mediante conductas inequívoca, cuando su comportamiento permita concluir de manera razonable que consintió el tratamiento de sus datos

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

personales. Se consideran conductas inequívocas, entre otras: (i) El diligenciamiento voluntario de formularios físicos o digitales. (ii) El envío de información a través de correos electrónicos o canales virtuales. (iii) El uso, navegación o interacción con plataformas, aplicaciones o portales digitales de la empresa. (iv) La suscripción o aceptación expresa de términos y condiciones asociados al tratamiento de datos.

Autorización para el tratamiento de datos personales sensibles

El tratamiento de datos sensibles se realizará cuando: (i) El titular haya otorgado autorización explícita y previa, salvo las excepciones legales. (ii) El tratamiento sea necesario para proteger un interés vital del titular y este se encuentre física o jurídicamente incapacitado. (iv) Exista un mando legal o judicial que lo autorice. La empresa informará de manera clara al titular que no está obligado a suministrar datos sensibles y adoptará medidas de seguridad reforzadas para garantizar su confidencialidad, integridad y acceso restringido.

Autorización inequívoca – Política de videovigilancia.

Seguridad Dissel Ltda. podrá realizar tratamiento de datos personales mediante sistemas de videovigilancia, con fines de seguridad, control, prevención de incidentes y protección de personas, bienes e instalaciones. La autorización se entenderá otorgada de forma inequívoca mediante: (i) Avisos visibles de videovigilancia ubicados en zonas de acceso. (ii) Información previa sobre la existencia y finalidad del sistema. (iii) Permanencia voluntaria del titular en áreas videovigiladas. Las imágenes y videos serán tratados bajo estrictas medidas de seguridad, acceso restringido y por el tiempo estrictamente necesario para cumplir las finalidades informadas.

Autorización para el tratamiento de datos biométricos

El tratamiento de datos biométricos se realizará cuando sea estrictamente necesario para fines de identificación, control de acceso, seguridad o cumplimiento legal. Dicho tratamiento requerirá autorización expresa y explícita del titular, salvo las excepciones previstas en la ley, y se realizará bajo protocolos de seguridad reforzada, minimización de datos y acceso restringido.


Deberes de los titulares e la información

Los titulares de los datos personales deberán:

- Suministrar información veraz, completa y actualizada.
- Conocer y cumplir la Política de Tratamiento de datos personales.
- Utilizar los canales oficiales para presentar consultas, reclamos o solicitudes.
- Abstenerse de divulgar información personal propia o de terceros sin autorización.
- Informar oportunamente cualquier error, incidente o uso indebido de la información.
- Respetar los lineamientos de confidencialidad y seguridad establecidos por la empresa.

15. Derechos de los titulares

De conformidad con lo establecido en la Constitución Política de Colombia, la Ley Estatutaria 1581 de 2012, el Decreto 1377 de 2013, el Decreto 1074 de 2015 y las demás normas que regulan el derecho fundamental de hábeas data, los titulares de los datos personales tratados por Seguridad Dissel Ltda. tienen los siguientes derechos:

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

- a. Conocer, actualizar y rectificar sus datos personales frente a Seguridad Dissel Ltda., en su calidad de Responsable del tratamiento, cuando estos sean parciales, inexactos, incompletos, fraccionados, induzcan a error o su tratamiento esté prohibido o no haya sido autorizado, salvo las excepciones legales.
- b. Solicitar prueba de la autorización otorgada para el tratamiento de sus datos personales, dicha autorización sea requerida conforme la ley.
- c. Recibir información, previa solicitud, respecto del uso que Seguridad Dissel Ltda., ha dado a sus datos personales, las finalidades del tratamiento y los terceros con los cuales se haya compartido, cuando a ello haya lugar.
- d. Presentar consultas y reclamos relacionados con el tratamiento de sus datos personales, de conformidad con los procedimientos establecidos en la presente política.
- e. Revocar la autorización y/o solicitar la supresión de sus datos personales cuando considere que el tratamiento no respeta los principios, derechos y garantías constitucionales y legales, siempre que no exista un deber legal o contractual que impida su eliminación.
- f. Acudir ante la Superintendencia de Industria y Comercio, para presentar quejas por presuntas infracciones a la normatividad en materia de protección de datos personales, previo agotamiento del trámite de consulta o reclamo ante Seguridad Dissel Ltda.

Ejercicio de los derechos por parte de los titulares

Seguridad Dissel Ltda. cuenta con una estructura administrativa, técnica, jurídica que le permite garantizar el ejercicio efectivo de los derechos de los titulares de datos personales, en cumplimiento de los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad. Para tal efecto, la empresa ha designado un área responsable de atender las solicitudes relacionadas con consultas, reclamos, actualización, rectificación, supresión y revocatoria de autorización en materia de tratamiento de datos personales.

Área designada

Oficial de protección de datos.

Canales de atención:


Correo electrónico: Calidad@dissel.com.co

Consultas

Los titulares de los datos personales podrán consultar la información personal que repose en cualquier base de datos de Seguridad Dissel Ltda. En consecuencia, la empresa garantizará el derecho de consulta, suministrando al titular la información contenida en el registro individual que este vinculada con su identificación.

Las consultas serán atendidas en un término de quince (15) días hábiles contados a partir de la fecha de su recibo. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado antes de su vencimiento, indicando los motivos de la demora y señalando la nueva fecha de respuesta, la cual no podrá superar los cinco (5) días hábiles adicionales.

Reclamos

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

Los titulares que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización, rectificación o supresión, o cuando adviertan el presunto incumplimiento de los deberes legales en materia de protección de datos, podrán presentar un reclamo ante Seguridad Dissel Ltda.

El reclamo deberá contener como mínimo:

- a. Identificación del titular.
- b. Documentos que acrediten la identidad o calidad en la que actúa.
- c. Descripción clara y precisa de los hechos que dan lugar al reclamo y de los datos respecto de los cuales se solicita el ejercicio del derecho.
- d. Dirección física o electrónica para recibir notificaciones.
- e. Documentos que se pretendan hacer valer.

Si el reclamo resulta incompleto, Seguridad Dissel Ltda., requerirá al interesado dentro de los cinco (5) días hábiles siguientes para que subsane la información. Transcurridos dos (2) meses sin respuesta, se entenderá que el reclamo ha sido desistido.

Los reclamos serán atendidos a un término máximo de quince (15) días hábiles contados a partir del día siguiente a su recepción. Cuando no sea posible atenderlos en dicho plazo, se informará al interesado antes de su vencimiento, indicando los motivos de la demora y la fecha de respuesta.

Supresión de datos

Los titulares tienen derecho a solicitar, en cualquier momento, la supresión total o parcial de sus datos personales de las bases de datos de Seguridad Dissel Ltda.

No obstante, la solicitud de supresión no procederá cuando:

- a. Exista un deber legal contractual que obligue a conservar la información (por ejemplo, relaciones laborales, obligaciones ante autoridades de vigilancia y control, SARLAFT, Seguridad privada, investigaciones, procesos judiciales o administrativos).
- b. La eliminación de los datos obstaculice actuaciones judiciales, administrativas o de control.
- c. La información sea necesaria para proteger intereses jurídicamente tutelados del titular o de terceros.

Revocatoria de la autorización


Los titulares podrán revocar la autorización otorgada para el tratamiento de sus datos personales, siempre que no exista una disposición legal o contractual que lo impida.

La revocatoria podrá ser:

- a) Total, cuando implique el cese completo del tratamiento de los datos personales.
- b) Parcial, cuando se refiera únicamente a determinadas finalidades, como actividades comerciales, publicitarias o de mercadeo, sin afectar otros tratamientos legítimos previamente autorizados.

Actualización de la información personal

La actualización de los datos personales de clientes, proveedores, trabajadores, contratistas, aliados estratégicos y demás titulares se realizará conforme a los procedimientos internos definidos en cada área, atendiendo criterios de periodicidad,

	SISTEMA INTEGRADO DE GESTION CALIDAD-CONTROL Y SEGURIDAD-SST	COD: OD-DE-10
	POLÍTICA TRATAMIENTO DE DATOS	VERSION: 1

necesidad, exactitud y seguridad de la información, así como las obligaciones legales aplicables al sector de Seguridad Privada y Vigilancia.

16. Vigencia y modificación de la política de Tratamiento de datos

La presente política de tratamiento de datos personales rige a partir de la fecha de su publicación, enero 30 de 2026..

Cualquier cambio en la política de tratamiento de datos, se comunicará de forma oportuna a los titulares de los datos a través de los medios habituales de comunicación.

Atentamente,

SEGURIDAD DISSEL LTDA.