POLÍTICA GENERAL PARA EL SISTEMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES

PESQUERA DISMARSUR S.A.S., identificada con NIT 901.125.725-7, (En adelante "la Sociedad"), en cumplimiento de sus obligaciones constitucionales, legales y reglamentarias, y en especial de lo ordenado en la Ley 1581 del 2012 y su Decreto Reglamentario 1377 del 2013, compilado en el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, Decreto 1074 del 2015, así como de las órdenes e instrucciones que sobre la materia ha dictado la Superintendencia de Industria y Comercio (En adelante "SIC"), como Autoridad Nacional de Protección de Datos Personales, con el presente documento hace pública la presente Política General de Tratamiento de Datos Personales, reconociendo la importancia de realizar el tratamiento de los datos personales de sus empleados, clientes, proveedores, contratistas, accionistas y en general de todas las personas que directa o indirectamente tienen relación con la Sociedad, bajo estrictos criterios de seguridad, privacidad, confidencialidad, libertad y transparencia.

I. OBJETIVO

La presente Política General del Sistema Integral de Gestión de Datos Personales, pretende definir las políticas y lineamientos a implementar por **PESQUERA DISMARSUR S.A.S.**, para la recolección, almacenamiento, uso, circulación y supresión de datos personales; reflejando así, una cultura de respeto a la protección de los mismos, con el fin de adoptar medidas dentro de la organización que permitan aumentar sus estándares de protección, para que de esta manera, sea garantizado a los empleados, clientes, proveedores, contratistas, accionistas y en general todas las personas que directa o indirectamente tienen relación con la Sociedad un tratamiento idóneo de su información personal y materializar el derecho que tienen todas las personas a conocer, actualizar y rectificar la información que se almacene sobre ellas en bases de datos o archivos.

II. ALCANCE Y OBLIGATORIEDAD

El presente sistema Integrado de Gestión de Datos Personales se aplicará de conformidad al desarrollo normativo al interior de la Sociedad, de las disposiciones legales y reglamentarias que rigen el tratamiento y protección de datos personales en Colombia, en consecuencia constituirá el criterio general para el tratamiento de los datos que se encuentren incluidos en las bases de datos, ficheros y archivos de la compañía para los

directivos, empleados, contratistas, titulares de los datos personales y cualquier otra persona que tenga relación directa o indirecta con la Sociedad.

Se exceptúan las bases de datos mantenidas en un ámbito exclusivamente personal o doméstico, es decir, de la vida privada o familiar de las personas naturales; así como las demás contenidas en el artículo 2 de la Ley 1581 de 2012.

La presente política constituye el marco general para el desarrollo de las políticas internas, protocolos, auditorias y procedimientos que permitan cumplir efectivamente los estándares de protección de datos personales exigidos por el ordenamiento jurídico colombiano. En consecuencia, las estipulaciones aquí consagradas son de estricto y obligatorio cumplimiento por parte de la sociedad **PESQUERA DISMARSUR S.A.S.,** identificada con NIT. 901.125.725-7, su representante legal, directivos, empleados, contratistas, proveedores y cualquier persona que tenga relación directa o indirecta con ésta.

III. MARCO JURÍDICO

El tratamiento de datos personales que realiza **PESQUERA DISMARSUR S.A.S.,** se soporta en los siguientes fundamentos jurídicos:

- Constitución Política de Colombia.
- Ley Estatutaria 1581 del 2012.
- Sentencia C – 748 del 6 de octubre del 2011.
- Decreto 1074 del 2015 “Decreto Único del Sector Comercio, Industria y Turismo”.
- Disposiciones de la Superintendencia de Industria y Comercio.

IV. RESPONSABLE DEL TRATAMIENTO

El responsable del tratamiento de datos personales es la sociedad **PESQUERA DISMARSUR S.A.S.**, identificada con NIT. 901.125.725-7.

DATOS DE CONTACTO:

Dirección: Carrera 9 número 17 – 43 en Neiva – Huila.

Teléfono: 3174417319

Correo electrónico: gerencia@dismarsur.com

V. DEFINICIONES

Para efectos de la presente política se adoptan las siguientes definiciones:

a) **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
b) **Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento.
c) **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.
d) **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.
e) **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.
f) **Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento.
g) **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
h) **Aviso de privacidad:** Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.
i) **Dato público.** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
j) **Datos sensibles.** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de

derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

k) **Transferencia:** La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

l) **Transmisión:** Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable.

VI. PRINCIPIOS RECTORES

Los principios que determinan el tratamiento de datos personales que realizará **PESQUERA DISMARSUR S.A.S**.,y que permitirán la aplicación e interpretación armónica de las disposiciones normativas que regulan la protección de datos personales en Colombia son:

a) **Principio de legalidad:** El Tratamiento a que se refiere la Ley 1581 del 2012 y que ha desarrollado **PESQUERA DISMARSUR S.A.S.,** a través del sistema de protección de datos personales, es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.

b) **Principio de finalidad:** El Tratamiento de datos personales debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, a través de la cual la sociedad **PESQUERA DISMARSUR S.A.S**., desarrolla su objeto social y la cual debe ser informada al Titular de los datos personales.

c) **Principio de libertad:** El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular de los datos personales. Estos no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

d) **Principio de veracidad o calidad:** La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Está prohibido a los empleados y contratistas de la Sociedad, el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

e) **Principio de transparencia:** En el tratamiento de datos personales debe garantizarse el derecho del titular a obtener del responsable o encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de sus datos personales, el tratamiento que se le han dado a los mismos y cualquier otra información directamente relacionada con estos y que sea solicitada por el titular o las personas legalmente habilitadas.

f) **Principio de acceso y circulación restringida:** El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la Ley 1581 del 2012. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la citada ley.

g) **Principio de seguridad:** La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

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

VII. TRATAMIENTO Y FINALIDADES

La sociedad **PESQUERA DISMARSUR S.A.S**., realizará el tratamiento de los datos personales incluidos en sus bases de datos, con el fin de desarrollar su objeto social.

El tratamiento de los datos personales por parte de la Sociedad se hará a partir de la recolección y almacenamiento en bases de datos y el uso en correspondencia con las finalidades señaladas en el acto de autorización. Para su registro, uso, consulta, modificación, supresión o cualquier otra operación relacionada con éstos, la Sociedad

garantizará las medidas de seguridad necesarias para el reconocimiento y respeto de los derechos de sus titulares.

El uso de los datos personales se hará, preferiblemente, a través de llamadas telefónicas, comunicaciones físicas a las direcciones de contacto y el envío de correos electrónicos, mensajes de datos y en general por cualquier medio de comunicación que permita el contacto efectivo con el titular de la información.

Las finalidades del tratamiento de datos personales que hace la Sociedad, atendiendo a la naturaleza de los datos y a sus titulares, son:

a) Registrar, controlar y gestionar el acceso de personas a las instalaciones físicas de la Sociedad, disminuyendo con ello riesgos de seguridad al personal y la protección a bienes e instalaciones de las mismas.
b) Gestionar el cumplimiento de las obligaciones sociales frente a los órganos internos de la Sociedad, frente a terceros y frente a las autoridades administrativas y judiciales.
c) Establecer, controlar y verificar el desarrollo de los procesos y actividades adelantadas por la Sociedad.
d) Cumplimiento de obligaciones constitucionales, legales y contractuales en desarrollo del objeto social.
e) Gestionar las denuncias, comentarios, quejas y reclamos que interpongan empleados, proveedores o terceros con relación directa e indirecta con la sociedad **PESQUERA DISMARSUR S.A.S.,** con miras a establecer criterios de responsabilidad corporativa, corregir y anular las malas prácticas que afecten la ética y transparencia corporativa.
f) Soportar el desarrollo de gestión, operaciones y procesos de la Sociedad a través de las herramientas y aplicaciones informáticas.
g) Evaluar el perfil laboral de los aspirantes con miras a la selección y vinculación de sus empleados supliendo las vacantes o requerimientos de personal.
h) Establecer registro, contacto y comunicación de accionantes, empleados, proveedores y personas de interés para el desarrollo del objeto social de la Sociedad.
i) Soportar documentalmente las actuaciones administrativas o judiciales que se adelanten por parte de la Sociedad.

j) Envío de propuestas técnicas y económicas, portafolio de servicios y cualquier otro documento tendiente a celebración de relaciones contractuales.
k) Envío de mercadeo, investigación, información estadística, y cualquier otra relevante que permita una comunicación efectiva con sus accionante, empleados, proveedores, y cualquier persona con la que tenga relación directa o indirecta.
l) Consulta de comportamiento financiero y crediticio, así como el consecuente reporte a las centrales de información en caso de incumplimiento de las obligaciones de carácter pecuniario adquiridas con la Sociedad.
m) Procesamiento contable, así como el de pagos y cobros por los servicios contratados por la Sociedad.
n) Recepcionar, tramitar y resolver los procedimientos de habeas data.
o) Cumplir cualquier requerimiento u orden de autoridades administrativas o judiciales en cumplimiento de sus obligaciones legales.
p) Transferencia o transmisión de los datos, cuando esto resulte necesario y se tenga la autorización expresa para el efecto.
q) Gestión administrativa de la Sociedad.
r) Gestión de cobros y pagos a cargo y en favor de la Sociedad.
s) Gestión de facturación.
t) Gestión de proveedores.
u) Gestión fiscal y contable de la Sociedad.
v) Gestión del talento humano de la Sociedad.
w) Gestión de la relación laboral y el bienestar social de los empleados.
x) Otras actividades acordes y necesarias en desarrollo del objeto social de la Sociedad.

VIII. INVENTARIO DE LAS BASES DE DATOS CON INFORMACIÓN PERSONAL

La organización debe conocer qué datos personales almacenan, cómo los utilizan y si realmente los necesitan, teniendo en cuenta la finalidad para la cual los recolectan, pues los Responsables y Encargados del Tratamiento sólo podrán recolectar, almacenar, usar o circular los datos personales durante el tiempo que sea razonable y necesario, de acuerdo con las finalidades que justificaron el Tratamiento, atendiendo a las disposiciones aplicables a la materia de que se trate ya los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.

Una vez cumplida la o las finalidades del Tratamiento y sin perjuicio de normas legales que dispongan lo contrario, el Responsable y el Encargado deberán proceder a la supresión de los datos personales en su posesión. No obstante, los datos personales deberán ser conservados cuando así se requiera para el cumplimiento de una obligación legal o contractual.

IX. CLASIFICACIÓN DE LAS CLASES DE DATOS RECOLECTADOS

1. **Datos de identificación:**

1.1 Públicos: Datos generales de la persona, familiares, beneficiarios o terceros.

- Nombre, apellido, tipo de identificación, número de identificación, fecha y lugar de expedición, estado civil, sexo, entre otros.

1.2 Semiprivados: Datos específicos de identificación de la persona.

- Firma, nacionalidad, datos de familiares, firma electrónica, documentos de identificación, fecha de nacimiento o muerte, edad, entre otros.

1.3 Sensibles: Datos biométricos de la persona y de descripción morfológica de la persona.

- Huella dactilar, ADN, iris geometría facial o corporal, fotografías, videos, formula dactiloscópica, voz, entre otros.
- Color de piel, color de iris, color y tipo de cabello, señales particulares, estatura, peso, complexión, entre otros.

2. **Datos de ubicación:**

2.1 Públicos: Datos de ubicación relacionados con la actividad comercial o profesional.

- Dirección, teléfono, correo electrónico, entre otros.

2.2 Privados: Datos de ubicación personal relacionados con actividad privada de las personas.

- Domicilio, teléfono, correo electrónico, entre otros.

3. **Datos sensibles:** Aquellos datos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación.

1. Datos relacionados con la salud y/o el estado de salud de la persona.

- En cuanto a órdenes y relación de pruebas complementarias como pruebas de laboratorio, imagen, endoscópicas, patológicas, estudios, entre otros. (No incluye resultados ni diagnósticos).
- Resultado de pruebas, laboratorios, estudios, diagnósticos médicos, generales o especializados, psicológicos o psiquiátricos, medicamentos y/o tratamientos médicos de cualquier tipo.

2. Datos relacionados con la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, religiosas, políticas.

3. Datos de preferencia, identidad y orientación sexual, origen étnico- racial, y otros de esta clase.

4. Datos en relación con población en condición vulnerable.

4. Datos socioeconómicos.

4.1 Semiprivados:

- Datos financieros, tributarios, crediticios y/o derechos de carácter económico de la persona.
- Historial laboral de la persona, experiencia laboral, cargo, fechas de ingreso y egreso, anotaciones y llamados de atención.
- Nivel educativo, capacitación y/o historial académico de la persona.
- Datos generales de afiliación y aportes al Sistema Integral de Seguridad Social (EPS, IPS, ARL, fechas de ingreso/retiro EPS, AF).

4.2 Privados: Estrato, propiedad de la vivienda, entre otros.

4.3 Públicos: Relacionados con la actividad económica de la persona.

Privados: Datos personales de acceso a sistemas de información.

- Usuarios, claves, IP, perfiles y entre otros.

5.2. Públicos: Datos sobre gustos e intereses particulares.

5.3 Públicos: Antecedentes judiciales y/o disciplinarios.

X. AUTORIZACIÓN

El tratamiento de los datos personales que haga **PESQUERA DISMARSUR S.A.S.,** deberá estar soportado en la autorización previa, expresa, informada y suficiente que obtenga del titular de los datos personales, a través de los distintos medios señalados en el ordenamiento jurídico. Ésta deberá documentarse y estar a disposición del titular y de la Superintendencia de Industria y Comercio.

La documentación de la autorización dependerá del sistema de recolección utilizado por la Sociedad según la naturaleza del dato a tratar y su titular. No obstante, por regla general será a través de formato físico preestablecido por **PESQUERA DISMARSUR S.A.S.**, adoptado e implementado por la Sociedad dentro del sistema general de protección de datos personales.

Cuando la finalidad del tratamiento de los datos personales varíe, deberá informarse al titular y obtenerse una nueva autorización en correspondencia con la nueva finalidad.

XI. CICLO DE GESTIÓN DE LOS DATOS PERSONALES

1. **Recolección:**

a) Finalidad y necesidad

En desarrollo de los principios de finalidad y libertad, deberá identificarse de acuerdo con el grupo de interés, en qué parte del procedimiento o actividad se obtienen los datos, así como la finalidad de la recolección de los mismos y una explicación sobre la necesidad de recolectar datos en cada caso.

La recolección de datos deberá limitarse a aquellos que son pertinentes y adecuados para la finalidad para la cual son recolectados o requeridos conforme a la normatividad vigente y a la Política de Protección de Datos Personales de **PESQUERA DISMARSUR S.A.S.**

En caso de haber cambios sustanciales en el contenido de la política del Tratamiento referidos a la identificación del Responsable y a la finalidad del Tratamiento de los datos

personales, los cuales puedan afectar el contenido de la autorización, se deberán comunicar estos cambios al Titular antes de o a más tardar al momento de implementar las nuevas políticas. Además, deberá obtener del Titular una nueva autorización cuando el cambio se refiera a la finalidad del Tratamiento. No se podrán utilizar medios engañosos o fraudulentos para recolectar y realizar Tratamiento de datos personales.

En los casos en los que no sea posible poner a disposición del Titular las políticas de Tratamiento de la Información, se deberá informar por medio de un Aviso de Privacidad al Titular sobre la existencia de tales políticas y la forma de acceder a las mismas, de manera oportuna y en todo caso a más tardar al momento de la recolección de los datos personales.

No obstante, cuando se recolecten datos personales sensibles, el Aviso de Privacidad deberá señalar expresamente el carácter facultativo de la respuesta a las preguntas que versen sobre este tipo de datos.

Finalmente, se deberá conservar el modelo del Aviso de Privacidad que se utilice para cumplir con el deber de dar a conocer a los Titulares la existencia de políticas del Tratamiento de la información y la forma de acceder a las mismas, mientras se traten datos personales conforme al mismo y perduren las obligaciones que de este se deriven.

Para el almacenamiento del modelo, se podrán emplear medios informáticos, electrónicos o cualquier otra tecnología que garantice el cumplimiento de lo previsto en la Ley 527 de 1999.

b) Autorización.

Salvo en los casos expresamente previstos en la ley, no se podrán recolectar datos personales sin autorización del Titular.

La Autorización del Titular no será necesaria cuando se trate de:

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

Aquellos datos o bases de datos que se encuentren a disposición del público pueden ser tratados por cualquier persona siempre y cuando, por su naturaleza, sean datos públicos.

La administración de datos semi - privados y privados requiere el consentimiento previo y expreso del titular de los datos, salvo en el caso del dato financiero, crediticio, comercial, de servicios y el proveniente de terceros países, el cual no requiere autorización del titular.

El Tratamiento de los datos sensibles está prohibido, a excepción de los casos expresamente señalados en el artículo 6 de la ley 1581 de 2012.

En el Tratamiento de datos personales sensibles, cuando dicho Tratamiento sea posible deberán cumplirse las siguientes obligaciones:

1. Informar al Titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento.
2. Informar al Titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, así como obtener su consentimiento expreso.

Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles.

c) Mecanismos para obtener la autorización.

Los mecanismos podrán ser predeterminados a través de medios técnicos que faciliten al titular su manifestación automatizada, por escrito, de forma oral o mediante conductas inequívocas del titular. En ningún caso el silencio podrá asimilarse a una conducta inequívoca.

d) Prueba de la autorización.

Los Responsables deberán conservar prueba de la autorización otorgada por los Titulares de datos personales para el Tratamiento de los mismos.

Seguridad de la Información:

a. **Confidencialidad:** Hace referencia a la protección de información cuya divulgación no está autorizada.

b. **Integridad:** La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.
c. **Disponibilidad:** La información debe estar en el momento y en el formato que se requiera, al igual que los recursos necesarios para su uso.

Calidad de la información:

a. **Efectividad:** La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.
b. **Eficiencia:** El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos.
c. **Confiabilidad:** La información debe ser la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones.

2. Medidas de seguridad:

La compañía implementará un Sistema de Gestión de Seguridad de la Información, adoptando medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros, evitando su adulteración, pérdida, consulta o acceso no autorizado o fraudulento, el cual contará con los siguientes ítems, a saber:

a. Conocimiento de dónde se almacenan los datos.
b. Conocimiento de la información según su necesidad y control de acceso a la información personal.
c. Adopción de política de seguridad específica para datos sensibles.
d. **Seguridad de la red**. Mecanismos de protección de las bases de datos como son herramientas actualizadas de firewall y un software antivirus.
e. **Respaldos.** Estrategias de respaldo múltiple que incluya respaldos en cinta fuera de línea y fuera de las instalaciones.
f. Inventario.
g. **Controles de seguridad en la tercerización de servicios**. Corresponde a aquellos controles implementados en los procesos o tratamientos de datos que se realizan a través de terceros ajenos a la organización. Con estos se deberán suscribir contratos de transmisión de datos personales.
h. **Acceso remoto.** Adopción de medidas que garanticen de forma confiable la consulta, uso o extracción de la información de manera remota.

i. **Monitoreo de consulta.** Efectuar trazabilidad o seguimiento de cualquier consulta que realice sobre la base de datos con información personal.
j. **Gestión de riesgos.** Implementación de herramientas que permitan y faciliten los procesos de prevención, mitigación y preparación de las capacidades de la organización para evitar, disminuir o transferir los efectos adversos o impactos negativos de las amenazas detectadas en un proceso de análisis del entorno durante las etapas del ciclo del dato y la naturaleza de los mismos.
k. **Protocolos de respuesta en el manejo de violaciones e incidentes.** Elaboración de protocolos de respuesta que anticipen riesgos y/o acciones que conlleven una vulnerabilidad de seguridad; previéndose junto con lo anterior, mecanismos para rendir informes internos y reportar incidentes de seguridad a titulares de la información, la Superintendencia de Industria y Comercio y la Alta Dirección.

De igual manera, se deberá comunicar de manera eficiente a los titulares afectados sobre el incidente ocurrido y las posibles consecuencias y proporcionar herramientas para minimizar el daño potencial o causado. La Ley 1581 de 2012 no hace distinción entre los incidentes que deben ser reportados a la Superintendencia, por lo que, independientemente de su impacto, deben reportarse a esta entidad todos los incidentes ocurridos, informando como mínimo:

1. El tipo de incidente ocurrido.
2. Fecha en que ocurrió.
3. Fecha en que se tuvo conocimiento del mismo.
4. La causal.
5. Tipo de datos personales comprometidos.
6. Cantidad de titulares afectados.

La información personal recolectada tendrá un tratamiento conforme a la finalidad de los datos y para el suministro de la información al titular, previa autorización; de la misma manera se podrá suministrar a los operadores autorizados para su administración, de manera verbal o escrita, o puesta a disposición de las siguientes personas y en los siguientes términos:

a. A los titulares, a los terceros debidamente autorizadas por estos o por la ley y a sus causahabientes o sus representantes legales.

b. A los usuarios de la información, dentro de los parámetros de la ley 1266 de 2008 Habeas Data.

c. A cualquier autoridad judicial, previa orden judicial.

d. A las entidades públicas o administrativas en el ejercicio de sus funciones legales o de orden judicial.

e. A los órganos de control y demás dependencias de investigación disciplinaria, fiscal, o administrativa, cuando la información sea necesaria para el desarrollo de una investigación en curso.

f. A otros operadores de datos, cuando se cuente con autorización del titular, o cuando sin ser necesaria la autorización del titular el banco u operador de datos de destino tenga la misma finalidad o una finalidad que comprenda la que tiene el operador que entrega los datos. Si el receptor de la información fuere un banco de datos extranjero, la entrega sin autorización del titular sólo podrá realizarse dejando constancia escrita de la entrega de la información y previa verificación por parte del operador de que las leyes del país respectivo o el receptor otorgan garantías suficientes para la protección de los derechos del titular.

3. Conservación y supresión:

La Sociedad como responsable del Tratamiento, solo podrá recolectar, almacenar, usar o circular los datos personales durante el tiempo que sea razonable y necesario, de acuerdo con las finalidades que justificaron el tratamiento, atendiendo a las disposiciones aplicables a la materia de que se trate y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.

Una vez cumplida la o las finalidades del tratamiento y sin perjuicio de normas legales que dispongan lo contrario, deberá proceder a la supresión de los datos personales en su posesión. No obstante, los datos personales deberán ser conservados cuando así se requiera para el cumplimiento de una obligación legal o contractual.

Sin perjuicio de lo anterior de acuerdo con las disposiciones de debida diligencia frente a los posibles riesgos en términos del Lavado de Activos y de la Financiación al Terrorismo, luego de terminada la relación comercial todos los registros necesarios sobre las transacciones, tanto locales como internacionales podrán estar por un periodo de al menos cinco (5) años, para que estas puedan cumplir con las peticiones de información emanadas de las autoridades competentes. Estos registros deben ser suficientes para permitir la

reconstrucción de transacciones individuales de manera tal que se ofrezca evidencia, de ser necesario, para procesamiento de una actividad criminal; una vez cumplida la o las finalidades, deberán proceder a la supresión de los datos personales en su posesión.

Por otro lado, por disposición expresa de la Superintendencia de Sociedades, con ocasión de la expedición y entrada en vigencia de la Ley 962 de 2005, específicamente su artículo 28, los comerciantes en general, tienen la obligación de conservar los libros y la documentación, por los medios que le facilita la ley, por un periodo mínimo de diez (10) años, término a partir del cual cesa la obligación; por ende, nada obsta para proceder a la su destrucción, sin perjuicio que con posterioridad decidan continuar conservándolos.

Una vez identificados los riesgos asociados con el tratamiento de datos, se deben implementar controles en cuanto a lo que se decida hacer finalmente con la información como eliminación (borrado seguro), destrucción o conservación, de manera que nunca se expongan a un uso no autorizado o fraudulento.

3. Revocatoria de la autorización y/o supresión del dato.

Los Titulares podrán en todo momento solicitar al responsable o encargado la supresión de sus datos personales y/o revocar la autorización otorgada para el Tratamiento de los mismos, mediante la presentación de un reclamo, de acuerdo con lo establecido en el artículo 15 de la Ley 1581 de 2012.

La solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el Titular tenga un deber legal o contractual de permanecer en la base de datos.

Se pondrán a disposición del Titular mecanismos gratuitos y de fácil acceso para presentar la solicitud de supresión de datos o la revocatoria de la autorización otorgada. Si vencido el término legal respectivo, el responsable y/o el encargado, según fuera el caso, no hubieran eliminado los datos personales, el Titular tendrá derecho a solicitar a la Superintendencia de Industria y Comercio que ordene la revocatoria de la autorización y/o la supresión de los datos personales. Para estos efectos se aplicará el procedimiento descrito en el artículo 22 de la Ley 1581 de 2012.

XII. INCIDENTES DE SEGURIDAD DE DATOS PERSONALES

Un Incidente de seguridad de datos personales se refiere a la violación de los códigos de seguridad, pérdida, robo y/o acceso no autorizado de datos personales que sean tratados bien sea por el Responsable del Tratamiento o por su Encargado.

a) **Causales de los incidentes:**

Fraude interno. Delito efectuado con la participación de los empleados o personas de confianza del Responsable o Encargado del Tratamiento, bien sea en forma directa o indirecta**.**

Fraude externo. Cualquier acto efectuado por una persona ajena al Responsable o Encargado del tratamiento, buscando acceder, apropiarse, causar adulteración o eliminación a los datos personales a los cuales, estos les realizan tratamiento.

Daños a activos físicos. Pérdida, deterioro o cualquier afectación de los datos personales, causados por daños a los activos físicos de los mismos, a saber:

- Daño físico en los computadores de la empresa, archivos físicos como papel, cintas, discos, etc., causados por cualquier tipo de incidencia como fenómenos naturales, accidentales o por problemas de orden público.

Falla de tecnología informática. Pérdida, indisponibilidad, adulteración o cualquier afectación de los datos personales, causados por fallas en la infraestructura tecnológica de uno u otro, a saber:

- Daño en el funcionamiento de los sistemas de información, daño en las redes de datos, problemas con los canales de transmisión de información, VPN, aplicaciones, etc.

Ejecución y/o administración de procesos. Pérdida, indisponibilidad, adulteración o cualquier afectación de los datos personales a los cuales el Responsable o Encargado realicen tratamiento, causados por fallas en la ejecución, aplicación y/o administración de procesos, protocolos, políticas de uno u otro, a saber:

- Toda vulneración que se detecte por la mala aplicación o ejecución de un procedimiento ya establecido, el cual debe estar documentado y llevar una trazabilidad de su correcta ejecución.

Falla por negligencia o actos involuntarios de los titulares. Pérdida, indisponibilidad, adulteración o cualquier afectación de los datos personales a los cuales el Responsable o Encargado realicen tratamiento, causados por negligencia o actos involuntarios del mismo titular, que puede ver afectados tanto sus propios datos como los de otros titulares.

b) Tipo de incidente de seguridad

Afecta la confidencialidad de los datos personales. Todos aquellos incidentes que afecten el principio de seguridad relacionado con la Confidencialidad de los datos personales, siendo ésta, la característica que evita la divulgación de la información a personas o procesos que no estén debidamente autorizados.

Afecta la disponibilidad de los datos personales. Todos aquellos incidentes que afecten el principio de seguridad relacionado con la Disponibilidad de los datos personales, que es la característica que garantiza el acceso a la información por las personas o procesos autorizados, siempre que sea requerida.

Afecta la integridad de los datos personales. Todos aquellos incidentes que afecten la Integridad de los datos personales, como aquella característica que garantiza que la información se mantenga, tal como fue recolectada o generada, sin alteraciones o modificaciones no solicitadas o autorizadas.

Afecta la confidencialidad y disponibilidad de los datos personales. Son aquellos incidentes en los cuales se afecta al mismo tiempo y de acuerdo con las definiciones anteriores los pilares de la seguridad de la información relacionados con la confidencialidad y disponibilidad de los datos personales.

Afecta la confidencialidad e Integridad de los datos personales. Son aquellos incidentes en los cuales se afecta al mismo tiempo y de acuerdo con las definiciones anteriores los pilares de la seguridad de la información relacionados con la confidencialidad e Integridad de los datos personales.

Afecta disponibilidad e integridad de los datos personales. Son aquellos incidentes en los cuales se afecta al mismo tiempo y de acuerdo con las definiciones anteriores los pilares de la seguridad de la información relacionados con la disponibilidad e Integridad de los datos personales.

- Acceso autorizado a la base de datos personales con adulteración de algunos o todos los datos personales encontrados en la misma y que para perpetrar el hecho, se realice cualquier acción en forma temporal o definitiva en la que se evite el acceso a la información del (los) titular (es) por parte de personas o procesos autorizados.

Afecta la confidencialidad, disponibilidad e integridad de los datos personales. Son aquellos incidentes en los cuales se afecta al mismo tiempo y de acuerdo con las

definiciones anteriores los pilares de la seguridad de la información relacionados con la confidencialidad, disponibilidad e integridad de los datos personales.

- Acceso no autorizado a la base de datos con información personal y adulteración de algunos o todos los datos personales encontrados en la misma y que para perpetrar el hecho, se realice cualquier acción en forma temporal o definitiva en la que se evite el acceso a la información del (los) titular (es) por parte de personas o procesos autorizados.

c) Medición y evaluación

Tiene por objetivo determinar la posibilidad de ocurrencia de los riesgos relacionados con el tratamiento de bases de datos personales y su impacto en caso de materializarse.

1. Control:

Se relacionan las acciones que se deben tomar para controlar y/o mitigar los riesgos a los que se ven expuestos los datos personales, con el fin de disminuir la posibilidad y/o las consecuencias de la materialización de los mismos.

El Sistema Integral de Gestión de Datos Personales exige una evaluación y revisión continúa de los controles que lo integran, con el fin de determinar la pertinencia y eficacia del plan de gestión. En consecuencia, el Oficial de Protección de Datos Personales será la persona encargada al interior de la organización de desarrollar un plan de supervisión y revisión anual que tome en cuenta las siguientes etapas:

- **Fase de diagnóstico:** Deberá evaluarse en qué estado de cumplimiento se encuentra la organización, acudiéndose, entre otras, a: (i) elaboración de auditorías internas; (ii) Identificación de debilidades en la atención de consultas y reclamos y; (iii) Revisión de las tendencias y obligaciones legales que surjan con ocasión a la protección de datos personales.
- **Fase de adecuación:** Consiste en determinar las acciones a implementar por la organización, en aras de hacer más efectivo el Sistema Integral de Gestión de Datos Personales.
- **Fase de implementación:** Es la materialización de los cambios que resulten pertinentes, según los resultados de las dos fases previas.

- **Fase de revisión:** Se deberá aplicar una revisión del Sistema Integral de Gestión de Datos Personales mínimo de manera anual, sin embargo, esto no es impedimento para realizar revisiones periódicos si se considera necesario.

2. **Procedimientos operacionales:**

Consisten en la elaboración de procedimientos que hagan alusión a la recolección y utilización de los datos personales al interior de la compañía. Por lo tanto, exige la definición de funcionarios, roles y actividades que deberán observarse para cumplir con las actividades propuestas.

3. **Monitoreo y evaluación:**

Consiste en el seguimiento constante para velar porque las medidas que se hayan establecido sean efectivas, para lo cual se deben implementar las siguientes acciones:

a. Contemplar un proceso de seguimiento efectivo que facilite la rápida detección y corrección de las deficiencias en la administración de los riesgos identificados.
b. Establecer indicadores que evidencien la efectividad del sistema de administración de riesgos adoptado.
c. Asegurar que los controles estén funcionando en forma oportuna, efectiva y eficiente.
d. Asegurar que los riesgos residuales se encuentren en los niveles de aceptación establecidos.
e. Llevar un registro de incidentes que contemple: Base de Datos y datos comprometidos, titulares, fecha del incidente y de descubrimiento, acciones correctivas realizadas y responsables.
f. Auditorías de seguridad. Establecer procedimientos automatizados que permitan evaluar la eficiencia y suficiencia de los controles implementados a un sistema de información mediante el cual se tratan datos personales para evitar su perdida, uso o acceso no autorizado o fraudulento, donde sea además posible evaluar el cumplimiento de requisitos, políticas y normas que específicamente apliquen.

XIII. DEBERES DE LA SOCIEDAD PESQUERA DISMARSUR S.A.S.

Cuando la Sociedad, de conformidad con los presupuestos jurídicos señalados en la Ley 1581 del 2012 y el capítulo 25 del Decreto 1074, realice tratamiento de datos personales en calidad de responsable, le será exigible el cumplimiento de las siguientes obligaciones:

a) Garantizar a los titulares de los datos personales objeto de tratamiento, en todo tiempo, el pleno y efectivo ejercicio del derecho de habeas data.
b) Solicitar y conservar soporte de la autorización otorgada por el titular para el tratamiento de sus datos personales.
c) Informar al titular de los datos personales sobre la finalidad de la recolección y los derechos que le asisten en virtud de la autorización otorgada.
d) Conservar los datos personales de los titulares bajo las condiciones de seguridad que impidan su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
e) Garantizar que la información que se suministre a los encargados del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
f) Actualizar la información, comunicando de forma oportuna al encargado del tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las medidas necesarias para que la información suministrada se mantenga actualizada.
g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al encargado del tratamiento.
h) Suministrar al encargado del tratamiento, según el caso, únicamente datos cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la Ley.
i) Exigir al encargado del tratamiento, en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular.
j) Recepcionar, tramitar y resolver las consultas y reclamos formulados en los términos señalados en la Ley 1581 del 2012, su decreto reglamentario y el manual de procedimientos de habeas data adoptado por **PESQUERA DISMARSUR S.A.S.**
k) Adoptar una política de seguridad y un manual de procedimientos de habeas data, para garantizar el adecuado cumplimiento de las obligaciones señaladas en la Ley y en especial para la atención de consultas y reclamos.
l) Informar al encargado del tratamiento cuando determinada información se encuentra en discusión por parte del titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
m) Informar, a solicitud del titular, sobre el uso dado a sus datos personales.

n) Informar a la Superintendencia de Industria y Comercio, como Autoridad Nacional de Protección de Datos Personales, cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

XIV. DEBERES DEL ENCARGADO

Cuando la sociedad **PESQUERA DISMARSUR S.A.S**., de conformidad con los presupuestos jurídicos señalados en la Ley 1581 del 2012 y el capítulo 25 del Decreto 1074, realice tratamiento de datos personales en calidad de encargado, le será exigible el cumplimiento de los anteriores deberes señalados.

Así mismo, con ocasión de la transmisión de datos personales regulada por el Capítulo 25 del Decreto 1074 del 2015, la Sociedad exigirá a sus contratistas y encargados del tratamiento de los datos personales, que además de cumplir con las obligaciones y requisitos establecidos en la Ley 1581 del 2012 para su tratamiento, cumpla especialmente con los siguientes deberes:

a) Garantizar a los titulares de los datos personales objeto de tratamiento por parte de la Sociedad en calidad de responsable, en todo tiempo, el pleno y efectivo ejercicio del derecho de habeas data.
b) Conservar los datos personales bajo condiciones de seguridad que impidan su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
c) Realizar oportunamente la actualización, rectificación o supresión de los datos personales, en los términos señalados en la Ley 1581 del 2012.
d) Actualizar la información reportada por la Sociedad dentro de los cinco (5) días hábiles contados a partir de su recibo.
e) Recepcionar, tramitar y resolver las consultas y reclamos formulados por los titulares de los datos personales, en los términos señalados en la Ley 1581 del 2012.
f) Adoptar una política de seguridad y un manual de procedimientos de habeas data, para garantizar el adecuado cumplimiento de las obligaciones señaladas en la Ley y en especial para la atención de consultas y reclamos.
g) Registrar en la base de datos la leyenda “reclamo en trámite” en la forma en que se regula en la Ley 1581 del 2012.

h) Insertar en la base de datos la leyenda “información en discusión judicial” una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
i) Abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
j) Permitir el acceso a la información únicamente a las personas previa y expresamente autorizadas.
k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio como Autoridad Nacional de Protección de Datos Personales.

PARÁGRAFO. En el evento en que concurran las calidades de responsable y encargado del tratamiento en la Sociedad o las funciones que desarrolle la sociedad no permitan establecer con claridad la condición en la que se actúa, le será exigible el cumplimiento de los deberes previstos para cada una de estas categorías.

XV. ÁREA RESPONSABLE DE HABEAS DATA

La sociedad **PESQUERA DISMARSUR S.A.S.,** de conformidad con su tamaño social, su capacidad institucional, la naturaleza y cantidad de datos personales respecto de cuales realiza tratamiento, designará al área de recursos humanos como la encargada de la adopción e implementación de esta Política General de Tratamiento de Datos Personales y del sistema de protección de datos personales. Para el debido cumplimiento de las obligaciones consagradas en la Ley 1581 del 2012 y el capítulo 25 del Decreto 1074 del 2015, así como de las órdenes e instrucciones que la Superintendencia de Industria y Comercio haga en la materia, esta área deberá dar trámite y resolución a todas las situaciones que se presenten en cuanto a lo consagrado en la normatividad vigente en el momento de su ocurrencia de tal situación.

XVI. DATOS DE NIÑOS, NIÑAS Y ADOLESCENTES

El Tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, de conformidad con lo establecido en el artículo 7° de la Ley 1581 de 2012 y cuando dicho Tratamiento cumpla con los siguientes parámetros y requisitos:

En caso de que en el desarrollo de su objeto social la sociedad **PESQUERA DISMARSUR S.A.S.,** llegara a realizar tratamiento de datos personales de niños, niñas y adolescentes, se aplicaran medidas especiales de seguridad en el tratamiento de esta información, tendiente a garantizar el debido tratamiento de los datos personales de este grupo poblacional, comprometiéndose a no poner en riesgo sus derechos fundamentales, y usar los datos recolectados únicamente cuando responda al interés superior de los menores.

La autorización previa, expresa e informada para el tratamiento de estos datos personales, será otorgada por representante legal del menor, atendiendo el concepto previo del menor, que será tenido valorado según su nivel de madurez sobre el tema.

XVII. PROTECCIÓN DE LOS DATOS PERSONALES

La sociedad **PESQUERA DISMARSUR S.A.S.,** ha implementado un sistema general de protección de datos personales que cumple con los estándares y requisitos exigidos por el ordenamiento jurídico para el tratamiento de esta información.

XVIII. PROCEDIMIENTOS DE HABEAS DATA

Los titulares de los datos personales podrán hacer valer sus derechos a través de comunicación física en la carrera 9 número 17-43 en la ciudad de Neiva – Huila o al correo electrónico gerencia@dismarsur.com . Las solicitudes que pretendan iniciar un procedimiento de habeas data deberán cumplir con los requisitos establecidos en los artículos 14 y 15 de la Ley 1581 del 2012.

XIX. DISPOSICIONES FINALES

La sociedad **PESQUERA DISMARSUR S.AS**., está facultada para modificar en cualquier momento la presente política general de tratamiento de datos personales. Cualquier cambio sustancial será comunicado al titular de los datos personales a más tardar al momento de entrada en vigor de las nuevas políticas.

La presente política general de tratamiento de datos personales entra en vigor a partir de mayo del año dos mil veintitrés (2023).

Atentamente,

PESQUERA DISMARSUR S.A.S.

NIT. 901.125.725-7