

océanos

MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DEL PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES.

REVISÓ: LUIS MAZINO ALVARINO CUDRIZ CARGO: ASESOR JURÍDICO	APROBÓ: FREDDY LÓPEZ CARGO: GERENTE ADMINISTRATIVO Y FINANCIERO	PRÓXIMA REVISIÓN FECHA:
FECHA: 09.11.23.	FECHA:	

OCEANOS S.A.

océanos
V.B.
DPTO. JURIDICO

MANUAL DE POLÍTICAS Y PROCEDIMIENTOS PARA EL TRATAMIENTO DE DATOS PERSONALES

Océanos S.A., sociedad comercial identificada con el NIT 890931654-0, con domicilio principal en Albornoz vía a Mamoñal N° 1-504, Cartagena-Bolívar-Colombia (en adelante, "Océanos" o la "Compañía"), reconoce la importancia de la seguridad, privacidad y confidencialidad de los datos personales de sus trabajadores, clientes, proveedores y en general, de todos sus agentes de interés respecto de los cuales ejerce tratamiento, por lo que en cumplimiento a los mandatos constitucionales y legales, ha implementado el siguiente documento que contiene el Manual de Políticas y Procedimientos Internos de Protección de Datos Personales y Privacidad.

CONSIDERACIONES PRELIMINARES

El Artículo 15 de la Constitución Política de la República de Colombia establece que cualquier persona tiene derecho a conocer, actualizar y rectificar los datos personales que existan sobre ella en bancos de datos o en archivos de entidades públicas o privadas. El artículo citado ordena a quienes tienen datos personales de terceros, respetar los derechos y garantías previstos en la Constitución cuando se recolecta, trata y circula esa clase de información.

Con el fin de desarrollar las garantías constitucionales a las que se refiere el artículo citado, así como el derecho a la información consagrado en el artículo 20 de la Constitución Política, el Congreso Nacional expidió la Ley Estatutaria 1581 de 2012, mediante la cual se establecen los principios y disposiciones que son aplicables al tratamiento de datos personales.

De conformidad con lo anterior, el tratamiento de datos personales realizado por Océanos se debe regir por el Régimen Colombiano de Protección de Datos Personales establecido por la ley citada, sus decretos reglamentarios y demás normatividad que la complementa, modifique o derogue. Para este fin, de acuerdo con lo establecido en el literal f) del Artículo 18 de la Ley 1581, Océanos adopta este Manual Interno de Políticas y Procedimientos para garantizar el adecuado cumplimiento del Régimen Colombiano de Protección de Datos Personales.

CONTROL DE CAMBIOS Y ACTUALIZACIONES

Versión	Cambios Introducidos	Aprobado por:
1.0	Documento inicial	Cargo: Asesor Jurídico Fecha: 2019/06/10 Firma:
2.0	<ul style="list-style-type: none"> • Actualización de roles y responsabilidades • Actualización de la política de tratamiento de datos personales • Actualización de atención de consultas • Actualización ciclo de vida del dato • Inclusión puntos 3, 5, 11 y 13 	Cargo: Asesor Jurídico Fecha: 2020/12/11 Firma:
3.0	<ul style="list-style-type: none"> • Actualización Bases de Datos Jurídicas. • Actualización de los responsables del comité de seguridad de la información y protección de datos. • Actualización Ciclo de vida del dato personal. • Actualización procedimiento de privacidad desde el diseño. • Inclusión procedimiento generación de reportes. • Ajuste en la estructuración del documento 	Cargo: Asesor Jurídico Fecha: 2023/05/09 Firma:

TABLA DE CONTENIDO

1. OBJETIVO DEL MANUAL.....	5
2. ALCANCE	5
3. MARCO NORMATIVO.....	5
4. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES.....	5
5. CRITERIOS PARA LA DEFINICIÓN DE BASES DE DATOS PERSONALES	7
6. ROLES Y RESPONSABILIDADES EN EL PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES DE LA COMPAÑÍA	10
6.1 RESPONSABILIDADES DE LA OFICINA DE PROTECCIÓN DE DATOS PERSONALES	11
6.2 RESPONSABILIDADES DE LA OFICINA DE PROTECCIÓN DE DATOS PERSONALES EN EL COMITÉ DE PROTECCIÓN DE DATOS	12
6.3 RESPONSABILIDADES DE LA OFICINA DE SEGURIDAD DE LA INFORMACIÓN EN PROTECCIÓN DE DATOS PERSONALES.....	12
6.4 RESPONSABILIDADES DEL COMITÉ DE PROTECCIÓN DE DATOS PERSONALES	13
6.5 RESPONSABILIDADES DE TODA LA ORGANIZACIÓN	16
7. DEBERES DE LA COMPAÑÍA CON RELACIÓN AL TRATAMIENTO DE DATOS PERSONALES....	17
7.1 OBLIGACIONES GENERALES	17
7.2 CONFIDENCIALIDAD	18
7.3 AUTORIZACIÓN DE LOS TITULARES.....	19
7.4 MEDIDAS CONTRACTUALES PARA LA PROTECCIÓN DE DATOS PERSONALES	20
7.5 TRANSFERENCIA NACIONAL DE DATOS PERSONALES	21
7.6 TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES	21
7.7 TRANSMISIÓN NACIONAL E INTERNACIONAL DE DATOS PERSONALES	22
7.8 PROCEDIMIENTO DE RELACIONAMIENTO CON TERCEROS	22
8. POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES OCÉANOS S.A.	24
9. PROCEDIMIENTO DE ATENCIÓN DE CONSULTAS Y RECLAMOS POR PARTE DE LOS TITULARES	36
10. PROCEDIMIENTO CICLO DE VIDA DEL DATO PERSONAL.....	44
11. PROCEDIMIENTO DE PRIVACIDAD DESDE EL DISEÑO.....	51
12. PROCEDIMIENTO GENERACIÓN DE REPORTES	58
13. DOCUMENTOS ADICIONALES	61

1. OBJETIVO DEL MANUAL

Definir los lineamientos generales para la aplicación, monitoreo, sostenimiento y mejora continua de las políticas y procedimientos internos asociados al Tratamiento de los Datos Personales en la Compañía.

2. ALCANCE

El presente Manual aplica para todas las actividades que desarrolle la Compañía y que conlleven el Tratamiento de Datos Personales en los términos del Régimen Colombiano de Protección de Datos Personales y, en particular, al Tratamiento de Datos Personales desarrollado en el ámbito nacional y a aquellas que generen flujos de dicha información hacia el exterior.

3. MARCO NORMATIVO



4. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES

Para el Tratamiento de Datos Personales, la Compañía aplicará los principios que se mencionan a continuación y que han sido previstos por el RCPDP como los lineamientos que deben orientar su recolección, manejo, uso, tratamiento, almacenamiento e intercambio:

- **Principio de legalidad en materia de Tratamiento de datos:**

El Tratamiento de los datos es una actividad reglada que debe sujetarse a lo establecido en la Ley 1581, en la política de protección de datos personales de la compañía y en las demás disposiciones que la desarrollen;

océanos

- **Principio de finalidad:**

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

- **Principio de libertad:**

El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento;

- **Principio de veracidad o calidad:**

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

- **Principio de transparencia:**

En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan;

- **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 Ley 1581 y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas/Entidades previstas por la Ley;

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 los disponga la Ley;

- **Principio de seguridad:**

La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

- **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

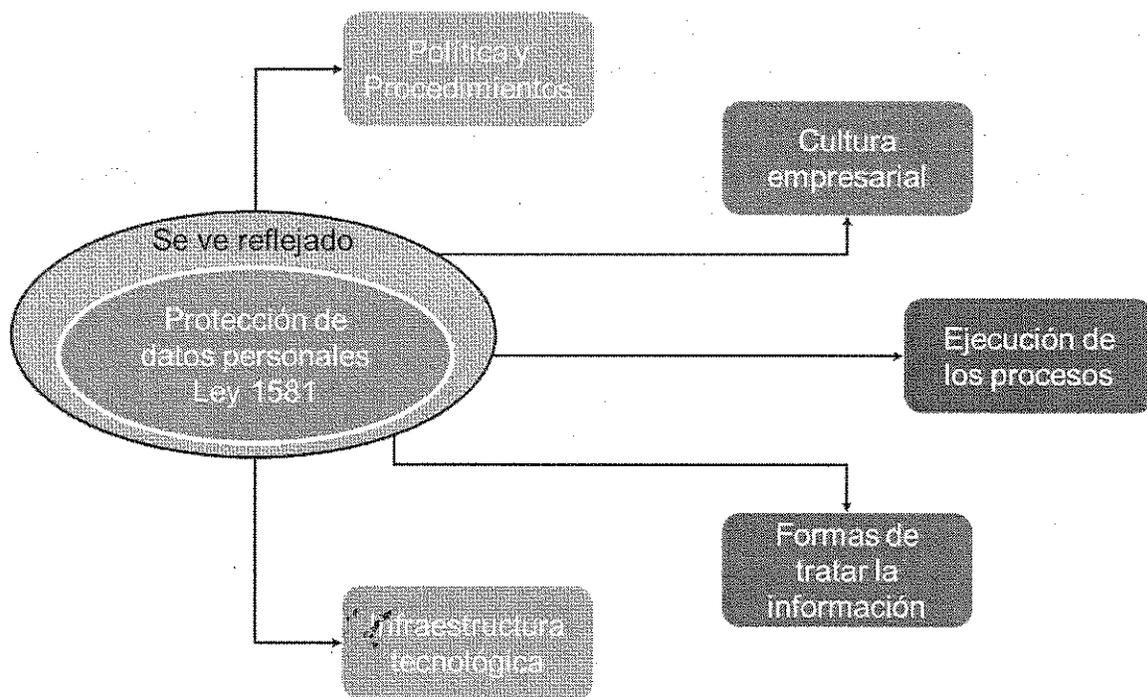
realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de sus actividades u objeto social.

5. CRITERIOS PARA LA DEFINICIÓN DE BASES DE DATOS PERSONALES

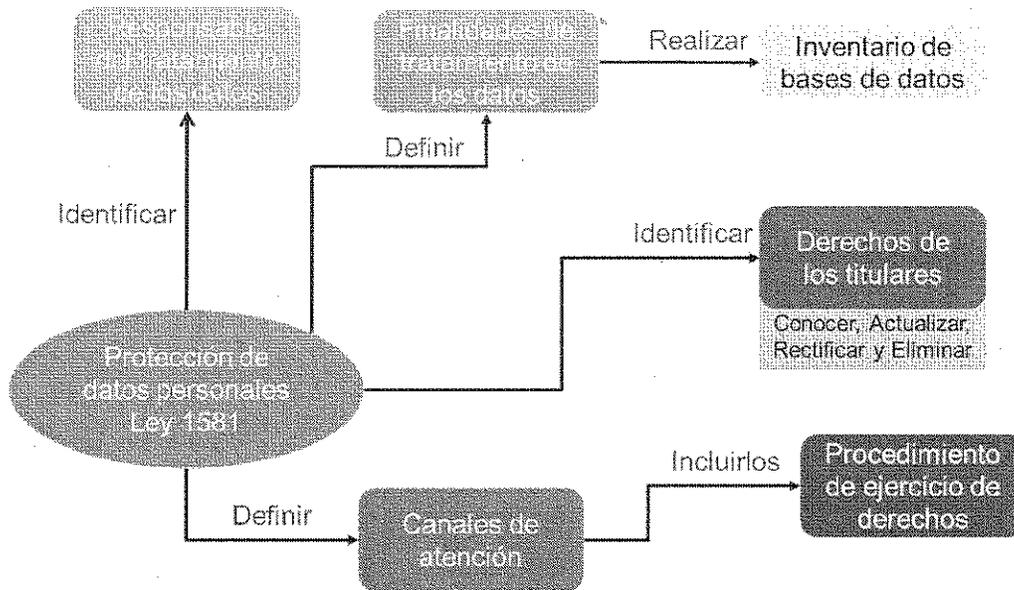
Como parte de los lineamientos para el adecuado tratamiento de los Datos Personales al interior de la Compañía, a continuación, se describen los criterios definidos por la Compañía para la conceptualización e identificación de las Bases de Datos que integran su ciclo de Tratamiento de información personal:

- ¿Qué son datos personales? Es la información que permite tu identificación.
- ¿Cuál es la importancia de los datos personales? Las finalidades de uso de los datos personales: Comerciales, contractuales, laborales y para cometer delitos como suplantación
- ¿Qué es la protección de datos personales? El derecho que posee cualquier persona de ejercer control y autoridad sobre su información, ya que, sobre ella, diferentes entidades realizan un tratamiento.

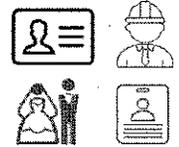
La implementación del RCPDP en una Organización se ve reflejada así:



A continuación, se presenta el flujo de actividades a realizar en la implementación del RCPDP:



A continuación, se presentan las definiciones de los tipos de datos:

Definición	Ejemplo	Donde
 Públicos: No requieren de una autorización por parte del propietario de la información para obtenerlos	 Nombre, Número de cédula, fecha de expedición profesión	 http://www.fosyga.in/fosyga/ NOTARIA TERCERA
 Semiprivados: Su conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector o grupo de personas en general	 BENTA BANCARIA	 Tarjetas de presentación
 Privados: relevantes solo para el Titular y se necesita autorización para ser recolectados, almacenados, usados, procesados, compartidos.		Bases de datos 
 Sensibles: Son aquellos que afectan la intimidad de la persona y su uso indebido puede generar discriminación Se requiere autorización para su tratamiento.	 SINDICATO	Hist.Clinica  Bases de datos

A continuación, se definen los criterios empleados al interior de la compañía para la clasificación de sus datos personales.

- **Bases de datos personales**

El Registro Nacional de Bases de Datos es el directorio público de las Bases de Datos sujetas a Tratamiento que operan en el país; que es administrado por la SIC.

Una Base de Datos es un conjunto organizado de datos personales objeto de Tratamiento. Todas las Bases de Datos que contengan datos personales cuyo Tratamiento automatizado o manual se realice por personas naturales o jurídicas, públicas o privadas, en el territorio colombiano (o fuera de él, si al Responsable o Encargado del Tratamiento les es aplicable la Ley colombiana en virtud de tratados internacionales). Es susceptible de registro ante la Superintendencia de Industria y Comercio.

- **Bases de datos digitales**

Estas Bases de Datos son creadas, ya sea por la utilización de sistemas de información, herramientas ofimáticas que utilizan las áreas de negocio, sistemas de video-vigilancia, sistemas biométricos y todo tipo de medio digital que permita almacenar información y realizar un tratamiento específico.

- **Bases de datos físicas**

Estas Bases de Datos son descentralizadas y su forma de recolección y almacenamiento es física (formato papel). Son creadas para una función específica de su trabajo con finalidades expresas y se almacenan en medios físicos (carpetas, A-Z, archivadores de escritorio, de pared, armarios de archivo, cuartos de archivo o archivo externo).

- **Bases de datos transaccionales**

Estas Bases de Datos son derivadas de bases de datos maestras las cuales son trabajadas en Excel, bases de datos transcritas de documentos físicos, información creada directamente de forma digital o documentación física recolectada directamente del titular y que son utilizadas para la realización de informes, análisis de datos, generar información para otras áreas u organizaciones con las que se tiene convenio, consolidación de información, estadística, transacciones y general, para las finalidades establecidas por la Compañía.

- **Bases de datos vigentes**

Bases de datos actuales, utilizadas para realizar el tratamiento de los datos personales de acuerdo con las finalidades establecidas en la política de protección de datos personales. Dentro de este grupo, puedo encontrar bases de datos digitales, físicas, transaccionales.

- **Bases de datos depuradas**

Son Bases de Datos que fueron depuradas del registro nacional de bases de datos (RNBD). La razón de su depuración obedece a que después de realizar el inventario de bases de datos, se identificó que dichas bases de datos: eran duplicadas, por ser archivos transaccionales compartidos de un área a otra; eran sub-bases de datos, es decir, eran extracciones de bases de datos maestras solamente

para consulta; no existían en el momento del inventario, ya que fueron bases de datos temporales que se usaron para una finalidad específica y fueron eliminadas o destruidas; no aplica para RNBD, ya que la información reportada contenía información restringida de la compañía pero no tenía datos personales que la constituyeran como tal en una base de datos personales.

- **Otras**

Bases de datos de contactos de Outlook, celulares y tarjeteros.

- Referente a los contactos de Outlook: No es una base de datos con datos estructurados, por estar en un medio de comunicación como el correo electrónico corporativo, el cual es un activo de la información, tiene las medidas de seguridad configuradas y establecidas por el proveedor de correo, y los datos contenidos corresponden a: cuentas de correo electrónico de colaboradores, clientes, proveedores, todos datos corporativos. Esta información se encuentra en los diferentes sistemas de información de la compañía y de manera estructurada.
- Referente a los contactos de celulares: No es una base de datos con datos estructurados. Son contactos de celular, en su gran mayoría de los mismos colaboradores ya que son cuentas corporativas.
- Referente a los contactos de tarjeteros: No es una base de datos con datos estructurados. Son tarjetas de presentación que corresponden a una información pública y temporal.

- **Bases de datos Jurídicas**

Bases de datos agrupadas por tipo de dato, finalidad y medio de almacenamiento. Estas bases de datos se reportaron en la RNBD y contienen las bases de datos vigentes.

Las agrupaciones definidas para la Compañía son las siguientes:

- CLIENTES - FÍSICA
- COLABORADORES - DIGITAL
- COLABORADORES – FÍSICA
- CONTROL COVID-19 - DIGITAL
- PROVEEDORES - DIGITAL
- PROVEEDORES - FÍSICA
- SEGURIDAD Y CONTROL DE ACCESO - DIGITAL
- SEGURIDAD Y CONTROL DE ACCESO - FÍSICA
- SISTEMA INFORMACIÓN SAP
- TERCEROS - DIGITAL
- TERCEROS – FÍSICA

6. ROLES Y RESPONSABILIDADES EN EL PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES DE LA COMPAÑÍA

En desarrollo de la normatividad vigente sobre el tratamiento de datos personales en Colombia y en particular de los artículos 23, 26 y 27 del Decreto 1377 de 2013, Océanos, como responsable del tratamiento de datos personales, designa como Oficina de protección de datos personales a su

departamento jurídico para que “Asuma la función de protección de datos personales” y “De tramite a los solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la ley 1581 de 2012 y realice las funciones consignadas en la guía de responsabilidad demostrada”.

La función de la Oficina de Protección de Datos personales es velar por la implementación efectiva de las políticas y procedimientos adoptados por la empresa, para dar cumplimiento a las normas, así como la implementación de buenas prácticas de tratamiento de datos personales. Teniendo como labor estructurar, diseñar, administrar, ejecutar, implementar y documentar el programa de gestión de protección de datos personales que permita a la Compañía el cumplimiento de las normas sobre protección de datos personales estableciendo y desarrollando controles, evaluaciones y revisiones periódicas y constantes del programa, haciendo especial énfasis en las medidas de seguridad, organizacionales y de cualquier otra naturaleza, que se implementen para la protección efectiva de los datos personales almacenados en las bases de datos de las que sea responsable la Compañía.

6.1 Responsabilidades de la Oficina de Protección de Datos Personales

- Realizar y actualizar la política de protección de datos personales y velar por su publicación y divulgación a las partes interesadas.
- Elaborar, revisar y actualizar los documentos de autorización de tratamiento de datos personales.
- Velar por el cumplimiento de la política de protección de datos personales por parte de los colaboradores en sus procesos diarios y que se tenga la respectiva autorización para el tratamiento de los datos.
- Participar en los proyectos de la Compañía para que desde su origen se diseñe con el componente de seguridad de la información y de protección de datos, identificando si es requerida una nueva base de datos, ciclo de vida del dato, encargados de la información, forma de captura del dato, finalidades, entre otros.
- Diseñar, ejecutar y actualizar el programa de protección de datos personales para la Compañía.
- Actualizar el inventario de las bases de datos personales de la Compañía y su registro ante la SIC (Superintendencia de Industria y Comercio)
- Revisar los contenidos de los contratos de transmisión y transferencia internacional de datos que se suscriban con Encargados o Responsables no residentes en Colombia y velar que ellos cumplan con las estipulaciones contractuales del encargo de tratamiento de datos personales.
- Revisar los contratos con los terceros en Colombia con los que se realice transmisión y transferencia de datos personales con el fin de dar cumplimiento a la normatividad vigente y a las políticas de la Compañía.
- Diseñar un programa de entrenamiento en protección de datos personales específico por el tipo de dato tratado en la Compañía, verificar que los colaboradores antiguos y nuevos participen en las capacitaciones brindadas.
- Impulsar una cultura de protección de datos dentro de la Compañía.
- Medir la participación y evaluar el desempeño en los entrenamientos de tratamiento de datos personales.
- Verificar la implementación de planes de auditoría interna que permitan comprobar el cumplimiento de sus políticas y procedimientos de tratamiento de datos personales.

- Acompañar, asistir y atender visitas y requerimientos que realice la Superintendencia de Industria y Comercio o la entidad competente en materia de tratamiento de datos personales.
- Realizar, ejecutar y actualizar el procedimiento de atención a consultas y reclamos de habeas data, y garantizar que se encuentren acorde a la normatividad vigente en la materia.
- Atender y gestionar las consultas y/o reclamaciones realizadas por el Titular o su representante.
- Realizar seguimiento y control a las actividades establecidas en la caracterización del proceso de protección de datos personales y cumplir con los indicadores establecidos.
- Realizar los reportes establecidos en la caracterización del proceso de protección de datos personales.
- Reportar a la Superintendencia de Industria y Comercio (SIC) las novedades del proceso de protección de datos: Incidentes, depuración de bases de datos, ejercicios de derechos de los titulares de los datos.
- Identificar y gestionar los riesgos, estableciendo los controles que permitan mitigarlos.
- Verificar de forma permanente los cambios en la normatividad aplicable a privacidad de los datos, informar los cambios que ocurran y evaluar el impacto de los mismos en la compañía y establecer el plan de implementación.

6.2 Responsabilidades de la Oficina de Protección de Datos Personales en el comité de protección de datos

- Reportar al comité de protección de datos personales, el estado cumplimiento del programa de privacidad, eventos o incidentes, nuevos riesgos identificados, cambios relevantes al proceso.
- Participar activamente en la definición de procedimientos que permitan hacer efectiva la Política Interna de Tratamiento de Datos de la Compañía, con el fin de dar cumplimiento a la normatividad vigente.
- Participar en la evaluación del nivel de riesgo aceptable relativo a los impactos para la Compañía por incidentes relacionados a Datos Personales.
- Informar tanto al comité de protección de datos personales como al comité de seguridad de la información, de los cambios en la normatividad aplicable al tratamiento de datos personales y las afectaciones al negocio en su contexto de operación para clasificar la información y seleccionar los mecanismos de control que permitan lograr el nivel de riesgo aceptable más rápido (más impacto, más probabilidades, más costo), con un sentido de negocio.

6.3 Responsabilidades de la Oficina de Seguridad de la Información en Protección de datos personales

El área de TI a quien se le ha asignado el rol de la Oficina de seguridad de la información participa en la implementación, diseño, evaluación y seguimiento de controles técnicos de seguridad para garantizar el cumplimiento de los principios de la información: Confidencialidad, integridad y disponibilidad.

Las responsabilidades descritas son en función de garantizar la protección de los datos personales de los cuales la Compañía es Responsable o Encargado.

- Identificar e implementar los controles técnicos para proteger la información, favoreciendo el cumplimiento de los requerimientos legales de privacidad, como también asegurar el

nivel de protección definido por la entidad y los requerimientos de las autoridades correspondientes.

- Apoyar la definición de iniciativas de mecanismos técnicos de cumplimiento de los requerimientos legales de protección de los Datos Personales.
- Definir y formalizar procedimientos para soportar la gestión de la seguridad de los sistemas de información:
 - a. RespalDOS de información.
 - b. Gestión y control de incidentes de seguridad de la información.
 - c. Destrucción y borrado de información.
 - d. Control de acceso a los recursos de infraestructura y datos personales.
 - e. Monitoreo de actividades en los recursos de infraestructura.
 - f. Control de vulnerabilidades técnicas.
- Participar en la definición del nivel de riesgo aceptable relacionado con el tratamiento de datos personales.
- Implantar los cambios tecnológicos que sugiera la normatividad referente a privacidad de la información y verificar las afectaciones al esquema tecnológico de la Compañía.
- Mantener actualizado el protocolo de respuesta a incidentes de seguridad de la información que comprometen datos personales.
- Entregar reporte de incidentes de seguridad de la información a la Oficina de protección de datos personales el cual informará a la Superintendencia de Industria y Comercio cuando lo requiera. Como mínimo debe informarse: el tipo de incidente, la fecha en que ocurrió, la fecha en la que se tuvo conocimiento del mismo, la causal, el tipo de datos personales comprometidos y la cantidad de titulares afectados.
- Llevar un registro de incidentes de seguridad de la información que comprometa datos personales, que contenga: Nombre de la base de datos, datos comprometidos, fecha del incidente, acciones correctivas, quién o cómo se originó el incidente, impacto

6.4 Responsabilidades del Comité de Protección de datos personales

A través de la definición del comité de protección de datos personales y seguridad de la información se busca integrar los requerimientos de privacidad y seguridad en la gestión operativa de la Compañía involucrando los líderes de los procesos, lo cual facilita el desarrollo de la cultura organizacional orientada a la protección de los datos personales y seguridad de la información y contribuye a la gestión efectiva de los riesgos.

El comité se reunirá con carácter ordinario una cada 3 meses y con carácter extraordinario, cuando la Oficina de protección de datos personales y/o el líder de seguridad de la información de la compañía lo considere pertinente, para tratar entre otros temas:

- Incidentes graves que puedan impactar la Compañía.
- Nuevas regulaciones o cambios en la legislación que requieran ser tratados en el comité.
- Proyectos nuevos de la Compañía con el fin de diseñar los proyectos con los componentes de seguridad y privacidad.
- Actividades de sensibilización

- Actualización documental
- Resolución de dudas referente al tratamiento de datos personales

De igual forma realizarán sesiones con las diferentes áreas de sus respectivas unidades de negocio máximo cada 3 meses para las siguientes actividades:

- Solicitar información de los proyectos en los que están trabajando las áreas o en los que van a iniciar para brindar desde el inicio el apoyo en PDP y Seguridad de la información.
- Ofrecer la resolución de inquietudes frente al tratamiento de datos y seguridad de la información.

Responsabilidades

En este documento se describen las responsabilidades de los integrantes del comité de privacidad y seguridad de la información de Océanos, el cual está integrado por los siguientes miembros:

- Gerencia Administrativa y Financiera
- Jefatura de Contabilidad
- El área jurídica como representante de la Oficina de protección de datos
- El área de TI como representante de la Oficina de seguridad de la información
- La consultoría externa, si se cuenta

Para la matriz RACI, se establecieron las siguientes siglas, las cuales se incluyen en la columna "Quién realiza":

- OPDP: Oficina de protección de datos interna.
- VCISO (Virtual CISO): Oficina externalizada de privacidad y seguridad conformada
- OSI: Oficina de seguridad de la información.
- GAF: Gerencia Administrativa y Financiera.
- JC: Jefatura de Contabilidad

Responsabilidad	Quién realiza	R	A	C	I	Observaciones
Facilitar la divulgación de la Política de Seguridad y Protección de datos personales	- GAF/JC		X			- A través de su apoyo y aprobación de las actividades que se realicen en torno a la divulgación de esta información. - Este respaldo se muestra llevando a la Alta Gerencia los temas tratados en el comité, facilitando la obtención de recursos para la realización de actividades.
	- OPDP - OSI	X				- Se realiza a través de las reuniones de comité primario, actividades coordinadas con RRHH y comunicaciones.
Promover la concienciación y formación de los colaboradores en	- OPDP - OSI	X	X			- Seleccionar los temas para capacitar a los colaboradores. - Establecer con RRHH cantidad y fechas de capacitaciones y los indicadores de medición

materia de seguridad de la información y protección de datos personales						- Identificar si se requiere contratar un servicio de capacitación.
	- VCISO	X				- B-SECURE se encargará de realizar las capacitaciones que sean acordadas en el alcance del servicio.
	- GAF/JC				X	- Ser informada de las actividades de sensibilización a realizar y obtener su apoyo al respecto.
Promover la cultura corporativa de protección de datos personales y seguridad de la información	- OPDP - OSI	X	X			- Coordinar con comunicaciones del Corporativo el despliegue de las piezas de sensibilización. - Realizar en conjunto con comunicaciones un programa de sensibilización donde se definan las fechas y el tipo de material a desplegar.
	- VCISO	X				- B-SECURE se encarga de entregar los textos de sensibilización a comunicaciones del Corporativo, quien se encarga de realizar el diseño gráfico de las piezas y hacer el despliegue de la información.
	- GAF/JC				X	- Ser informada de las actividades de sensibilización a realizar y obtener su apoyo al respecto.
Realizar seguimiento al desarrollo del programa de protección de datos personales y seguridad de la información	- GAF/JC - OPDP - OSI		X			- En las sesiones del comité se debe hacer seguimiento a las actividades del cronograma.
	- OPDP - OSI	X				- Cumplir con los compromisos propuestos por la oficina externa
	- VCISO	X				- Realizar las actividades propuestas en el cronograma, realizar actividades en conjunto con las personas de OPDP y OSI.
Asesorar a las Gerencias en los cambios y desarrollos de innovación para garantizar el cumplimiento de la política de privacidad y seguridad de la información.	- OPDP - OSI	X	X			- Coordinar con las áreas correspondiente, las actividades propuestas por VCISO.
	- VCISO	X			X	- Informar a las personas del OPDP y OSI acerca de los cambios en la legislación relacionada con protección de datos personales y que afecte las actividades de la compañía. - Referente a los cambios relacionados con L1581, proponer las acciones a realizar
	- GAF/JC			X	X	- Las personas de OPDP y OSI deberán informar con la GFA acerca de las actividades a realizar y consultar si es requerido cuando las actividades tengan un impacto por fuera de su alcance.
Apoyar la implantación de controles para la mitigación de riesgos de seguridad de información y protección de datos personales						
	- OPDP - OSI	X	X			- Implementar los controles en temas de privacidad y seguridad acordados entre el VCISO y las personas del OPDP y OSI. - Para la implementación de los controles se requiere apoyo de la gerencia y definir la manera de implementación. - Se requiere trabajo colaborativo con las áreas correspondientes.
	- VCISO	X				- Proponer controles de seguridad y privacidad. - Documentar los controles de seguridad y privacidad.

	- GAF/JC				X	- Informar a la Gerencia Financiera y administrativa el avance de la implementación de los controles y si se requieren recursos para ello.
Establecer los lineamientos de respuesta a cualquier requerimiento realizado por la Superintendencia de Industria y Comercio sobre la implementación del sistema de PDP y SI	- OPDP	X	X			- Ante un requerimiento de la SIC, se debe revisar el tipo de requerimiento, recolectar la información solicitada, establecer los términos de la respuesta
	- OSI				X	- Se debe notificar a la Oficina de seguridad de la información, en caso de que se requiera de su intervención.
	- GAF/JC			X	X	- Se debe notificar y consultar a la Gerencia Financiera y Administrativa acerca del requerimiento, el impacto, el alcance, la respuesta a entregar y consultar la forma en que se debe comunicar (si es requerido) el requerimiento a los interesados internos y externos.
	- VCISO			X		- Apoyar con la respuesta a la SIC, reunir la documentación requerida y actualizarla si es necesario.
Evaluar los impactos que traerán los cambios organizacionales, los nuevos proyectos o el diseño de nuevos servicios a la protección de datos personales y la seguridad de la información	- OPDP - OSI	X				- Frente a los proyectos nuevos o en curso que tenga la Compañía, identificar si hay tratamiento de datos personales y/o componentes de seguridad de la información que requieran ser revisados para que, desde el diseño o concepción del proyecto, se tenga cumplimiento en ambos frentes (privacidad y seguridad). - Notificar al VCISO para que realice la evaluación de los riesgos.
	- VCISO	X				- Realizar la evaluación de los riesgos de los nuevos proyectos que involucren temas de privacidad y/o seguridad de la información. - Proponer controles de seguridad.
	- GAF/JC				X	Ser informada de los nuevos proyectos, riesgos y controles implementados.

A continuación, se establece la correspondencia de las iniciales de la palabra RACI

- **Responsible (Responsable) - R:** Esta persona realiza la tarea o entrega.
- **Accountable (Autoridad) - A:** No harán el trabajo, pero son responsables de asegurarse de que esté finalizado.
- **Consulted (Consultado) - C:** Esta persona, rol o grupo proporcionará información útil para completar la tarea o entrega.
- **Informed (Informado) - I:** Estas personas o grupos se mantendrán al tanto de la tarea o entrega.

6.5 Responsabilidades de toda la Organización

- Conocer, Aceptar, comprender y aplicar las políticas de Protección de Datos Personales y Seguridad de la Información.
- Recolectar siempre la autorización para el tratamiento de datos por parte del Titular.
- Informar a la Oficina de Protección de Datos personales sobre los incidentes que ocurran en el tratamiento de los datos, así como informar al área de TI sobre incidentes de seguridad de la información.
- Verificar la identidad de todas aquellas personas, a quienes se les entrega información vía telefónica, correo electrónico o por correo certificado, entre otros.
- Hacer uso responsable y adecuado de los recursos tecnológicos que provee la compañía.
- Asegurarse de ingresar información adecuada a los sistemas de información.
- Proporcionar el adecuado tratamiento a los datos personales según su clasificación y en general a la información a su cargo.
- Remitir las consultas o reclamos a la Oficina de Protección de Datos personales de su Unidad de Negocio
- En cada nuevo proyecto, involucrar la Oficina de protección de datos personales y la Oficina de Seguridad de la Información, para que apoyen en la construcción de un proyecto seguro y en cumplimiento de la Ley.
- Utilizar los datos personales a su cargo, únicamente para las finalidades autorizadas.
- Transferir o transmitir la información solo cuando sea estrictamente necesario y autorizado.
- Asistir a las capacitaciones.

7. DEBERES DE LA COMPAÑÍA CON RELACIÓN AL TRATAMIENTO DE DATOS PERSONALES

7.1 Obligaciones Generales

La Compañía tiene presente que los Datos Personales son de propiedad de las personas a las que se refieren y solamente ellas pueden decidir sobre los mismos y, por tanto, hará uso de dichos datos solamente para las finalidades para las que se encuentra debidamente facultado y respetando, en todo caso, el RCPDP.

La Compañía atenderá los deberes previstos para los Responsables y Encargados del Tratamiento, contenidos en el RCPDP, a saber:

- Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- Solicitar y conservar, en las condiciones previstas en la ley, copia de la respectiva Autorización otorgada por el Titular.
- Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la Autorización otorgada.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- 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 demás medidas necesarias para que la información suministrada a este se mantenga actualizada.

- Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.
- Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la ley.
- Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
- Tramitar las consultas y reclamos formulados en los términos señalados en la Ley.
- Adoptar un Manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la Ley y en especial, para la atención de consultas y reclamos.
- 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.
- Tener un programa integral de protección de datos personales en la Compañía.
- Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

7.2 Confidencialidad

La Compañía garantiza y exige a toda persona que intervenga en cualquier fase del Tratamiento de Datos Personales el respeto de los mismos y el deber de guardarlos y mantener estricta confidencialidad de estos, obligaciones que subsistirán aún después de finalizar sus relaciones contractuales con la Compañía. El incumplimiento del deber antes enunciado se tendrá como un incumplimiento de las obligaciones laborales a cargo del respectivo trabajador.

Los trabajadores o cualquier tercero vinculado directa o indirectamente a la Compañía, deberán abstenerse de realizar sin autorización previa y por escrito de la Oficina de Protección de Datos Personales, cualquier iniciativa o actividad que involucre el uso de su nombre, enseña, razón social, símbolo, logo símbolo, marca o cualquier otro signo distintivo que impliquen el tratamiento de Datos Personales. Cualquier actividad o iniciativa que se adelante sin el cumplimiento del presente requisito será responsabilidad exclusiva de su(s) promotor(es) y no generará efectos, compromisos o responsabilidad alguna para la Compañía.

La presente disposición no aplicará para las actividades y/o gestiones de iniciativa institucional de la Compañía, las cuales en todo caso estarán sujetas al cumplimiento de las disposiciones del RCPDP y en particular, las del presente Manual.

La Compañía se abstendrá de publicar o divulgar mediante internet o cualquier otro medio masivo de comunicación, Datos Personales Sensibles de los Titulares respecto de los cuales ejerce Tratamiento, excepto en aquellos casos en los que se asegure que el acceso es técnicamente controlable para brindar un conocimiento restringido solo para los Titulares o terceros autorizados conforme a los términos legales y en aquellos casos en los que la Ley así lo requiera. De igual forma, la Compañía se abstendrá de divulgar o publicar información de carácter discriminatorio, ofensivo o que pueda afectar las particulares condiciones de vulnerabilidad o indefensión del Titular.

7.3 Autorización de los titulares

Cuando se trate de datos diferentes a los de naturaleza pública, definidos en el numeral 2 del artículo 3 del Decreto Reglamentario 1377 de 2013 o aquellos datos cuya recolección sea obligatoria por Ley, la Compañía solicitará la Autorización previa, expresa e informada para el Tratamiento de Datos Personales por cualquier medio que permita ser utilizado como prueba. Según el caso, dicha Autorización puede ser un documento amplio con la descripción de todas las finalidades, un formato donde de manera previa, se incluya la autorización, en el evento en que se capturen datos de manera masiva para una actividad puntual, Avisos de privacidad en las porterías de ingreso a las instalaciones, Aviso de privacidad para los eventos realizados por la compañía y otros que se requieran según el caso.

Cualquier duda en relación con el medio y/o documento en el cual se solicita la Autorización será aclarada por la Oficina de Protección de Datos Personales de la Compañía.

Se encuentran legitimados para otorgar la Autorización:

- El Titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que la Compañía ponga a su disposición.
- Los causahabientes del Titular, quienes deberán acreditar tal calidad.
- El representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.
- La Autorización también podrá darse cuando se den casos de estipulación a favor de otro o para otro.

Las Autorizaciones implementadas por la Compañía precisan a los Titulares:

- El Tratamiento al que serán sometidos sus Datos Personales y la finalidad específica del mismo.
- El carácter facultativo de las respuestas a las preguntas cuando estas versen sobre Datos Personales Sensibles o Datos Personales de menores de 18 años.
- Los derechos que le asisten como Titular previstos en el RCPDP.
- Correo electrónico, página web y en algunos documentos está la dirección física de la Compañía.

En adición a lo anterior y para el caso de los Datos Personales Sensibles se informará al Titular cuales de los datos que sean objeto de tratamiento, son sensibles.

Cada una de las áreas encargadas de la obtención de las Autorizaciones, deberá dejar prueba que demuestre el cumplimiento de la obligación de informar y obtener el consentimiento del Titular. Si el Titular solicita copia de la Autorización, la Compañía se encuentra obligada a suministrar dicha copia dentro de los términos previstos en la ley para el efecto.

La Autorización puede constar en un documento físico, electrónico, mensaje de datos, Internet, Sitios Web, o en cualquier otro formato que permita garantizar su posterior consulta, o mediante un mecanismo técnico o tecnológico idóneo, que permita manifestar u obtener el consentimiento vía clic o doble clic, mediante el cual se pueda concluir de manera inequívoca, que, de no haberse surtido una conducta del titular, los datos nunca hubieren sido capturados y almacenados en la base

de datos. La Autorización será generada por la Compañía y será puesta a disposición del Titular con antelación y de manera previa al tratamiento de sus datos personales.

La Compañía utilizará los mecanismos con que cuenta actualmente, e implementará y adoptará las acciones tendientes y necesarias para mantener registros o mecanismos técnicos o tecnológicos idóneos de cuándo y cómo obtuvo autorización por parte de los Titulares de Datos Personales para el Tratamiento de los mismos. Para dar cumplimiento a lo anterior, se podrán establecer archivos físicos o repositorios electrónicos realizados de manera directa o a través de terceros contratados para tal fin.

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

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

7.4 Medidas contractuales para la protección de datos personales

En los contratos laborales, la Compañía ha incluido cláusulas de confidencialidad, así como la autorización de tratamiento de datos personales relacionados con la ejecución del contrato, lo que incluye la facultada de recolectar, modificar o corregir, en momentos futuros, datos personales del Titular y sus beneficiarios y causahabientes. También ha incluido la autorización para que algunos de los Datos Personales puedan ser entregados o cedidos a terceros, para las finalidades descritas en el documento de autorización.

Referente a las relaciones contractuales con proveedores, la Compañía ha incluido cláusulas para asegurar el adecuado Tratamiento de los Datos Personales que, con ocasión de sus relaciones contractuales, sean transferidos o transmitidos entre ellos, quedando excluida de esta autorización, los datos de persona jurídica y su representante legal y los datos recolectados de fuentes públicas.

Respecto de terceros que actúen como Encargados del Tratamiento de datos personales de la Compañía, sus contratos incluirán cláusulas que precisan los fines y los Tratamientos autorizados y delimitan de manera precisa el uso que estos terceros le pueden dar a aquellos, así como las obligaciones y deberes establecidos en el RCPDP para garantizar en todo momento la confidencialidad, integridad y disponibilidad de los Datos Personales sujetos a Tratamiento.

Respecto de terceros que actúen como Responsables del Tratamiento de datos personales, es decir, a quienes se les realice transferencia o cesión de los datos, se garantizará que dichos datos cuentan con la debida autorización por parte del Titular de los mismos para ser transferidos, adicionalmente en el contrato, se indicarán las bases de datos que serán transferidas y que el Responsable (Cesionario) deberá informar al Titular de los datos, acerca del tratamiento de los mismos. La transferencia de los datos se realizará a empresas que cumplan con la LEPDP (Ley Estatutaria de Protección de Datos).

7.5 Transferencia nacional de datos personales

Las actividades de la Compañía que impliquen transferencia de Datos personales a otras Compañías dentro del país se regirán bajo las siguientes condiciones:

La Transferencia de Datos Personales solamente se realizará cuando exista Autorización correspondiente del Titular.

El Responsable de los datos, en este caso llamado contractualmente como Cesionario, deberá contar con una Política de protección de datos personales y los medios para garantizar un adecuado tratamiento de los mismos, cumpliendo con los principios de seguridad de la información: Confidencialidad, Integridad y Disponibilidad y con los demás señalados en el Artículo 4 de la Ley 1581 de 2012.

Es deber del Responsable (Cesionario), cumplir con la LEPDP (Ley Estatutaria de Protección de Datos) e informar al Titular de los datos, acerca de las finalidades de uso de los datos, cambios en su política de tratamiento de datos personales, canales de atención y responder sobre las consultas o reclamos que se generen por el tratamiento de los mismos.

7.6 Transferencia internacional de datos personales

Las actividades de la Compañía que impliquen la transferencia de Datos Personales a terceros países se sujetarán a las siguientes condiciones:

La Transferencia de Datos Personales a terceros países solamente se realizará cuando exista Autorización correspondiente del Titular y, en el evento en que el receptor se encuentre en un país que no proporcione un cierto nivel de protección, se requiere previa Autorización de la Delegatura de Datos Personales de la SIC.

Se considera Transferencia internacional cualquier Tratamiento que suponga el traslado de datos fuera del territorio colombiano, para que los datos sean tratados bajo las finalidades del Responsable en el País en que éste realice dicho tratamiento.

Asimismo, se debe obtener la Autorización previa del Delegado de Protección de Datos Personales de la Superintendencia de Industria y Comercio, cuando se tenga previsto realizar Transferencias internacionales de datos a países que no proporcionan un cierto nivel de protección. Esta autorización sólo podrá ser otorgada si se obtienen garantías adecuadas, como los contratos basados en las cláusulas tipo aprobadas por la SIC.

La Transferencia internacional de Datos Personales se podrá realizar mediante solicitud de la Compañía, estableciendo la finalidad, los Titulares, los Datos Personales objeto de Transferencia y la documentación que incorpore las garantías exigibles para la obtención de la Autorización, en la que conste una descripción de las medidas de seguridad concretas que van a ser adoptadas, tanto por el Responsable o Encargado de los datos en su lugar de destino.

La Compañía no solicitará la Autorización cuando la Transferencia internacional de Datos Personales se encuentre amparada en alguna de las excepciones previstas en el artículo 26 de la Ley 1581 de 2012.

7.7 Transmisión nacional e internacional de datos personales

Se entiende transmisión de datos personales a la relación entre Responsable y Encargado de la información, siendo este último, quien realizará un tratamiento de los datos personales de acuerdo con las finalidades establecidas por el Responsable de los datos.

Conforme reza en los artículos 24 y 25 del Decreto 1377 de 2013, la transmisión de datos personales no requiere ser informada al Titular, siempre que exista un contrato entre Responsable y Encargado, donde se indique:

- Finalidades del tratamiento de los datos
- Obligaciones del Encargado de los datos para con el Titular y el Responsable
- La obligación del Encargado de Salvaguardar las bases de datos y mantener la confidencialidad de la información.

La transmisión de datos personales puede darse en dos formas:

- La empresa que tiene los datos (el Responsable de los datos) le transmite la información al contratista (Encargado).
- El contratista (Encargado) captura los datos por encargo del Responsable y se los transmite a éste.

7.8 Procedimiento de relacionamiento con terceros

En línea con sus políticas y disposiciones internas en materia de protección de Datos Personales, la Compañía propenderá por vincularse o relacionarse comercialmente con aquellos terceros que reflejen su compromiso por la observancia del RCPDP en su respectiva operación: Para ello, la Compañía tendrá en cuenta el siguiente procedimiento general para el relacionamiento con terceros en el marco de su "diligencia demostrada" en materia de protección de los Datos Personales:

- a. De manera previa al relacionamiento con un tercero que implique Tratamiento, el área responsable, en coordinación con la Oficina de Protección de Datos Personales, revisarán los datos que serán objeto del contrato con el tercero implicado:
 - Tipos de datos objeto del contrato;
 - Finalidades del tratamiento de los datos;
 - Tipo de procesamiento que se le dará a los datos;
 - Cantidad de datos;
 - Formato de los datos: físico y/o digital;
 - Medios de Transmisión o Transferencia;
 - Medidas de seguridad para los medios de transmisión o transferencia;

- Medidas de seguridad para el almacenamiento de los datos, por parte del tercero;
 - Supresión o inactivación de los datos personales.
- b. En coordinación con la Oficina de Protección de Datos Personales y el área responsable, procederán a la realización de las verificaciones y controles aplicables según la categoría correspondiente, cuyo propósito será analizar el adecuado nivel de cumplimiento del RCPDP por parte del tercero antes de formalizar su vínculo o relacionamiento contractual.

Los mencionados controles o verificaciones del cumplimiento tendrán en cuenta los siguientes aspectos generales:

- Existencia política de tratamiento de datos personales.
 - Designación de la Oficina de privacidad.
 - Existencia de canales para la atención de Consultas y Reclamos en materia de protección de Datos Personales.
 - Existencia de controles de seguridad de la información.
 - Constancia de la realización o actualización del Registro Nacional de Bases de Datos Personales.
 - Existencia de solicitudes de Autorización para el Tratamiento de los Datos Personales asociadas al objeto del vínculo jurídico o comercial con el tercero, entre otros.
- c. Verificado el adecuado cumplimiento del RCPDP por parte del tercero, la Compañía procederá a realizar los trámites de formalización del vínculo contractual, estableciendo las respectivas coberturas legales asociadas con:
- Conocimiento, aceptación y aplicación de la Política de Tratamiento de Datos Personales de la Compañía por parte del tercero.
 - Facultad de la Compañía de supervisar el cumplimiento de las obligaciones del RCPDP por parte del tercero.
 - Aceptación y firma de los siguientes documentos:
 - Acuerdo de confidencialidad;
 - Cláusula de tratamiento de datos personales;
 - Cláusula / contrato de encargo / transferencia de datos personales.
- d. Si como resultado de las verificaciones y controles previos de debida diligencia se evidencia que el tercero no cumple con un adecuado nivel de cumplimiento del RCPDP, la Oficina de Protección de Datos Personales, en coordinación con área respectiva, definirán un plan de acción conjunto con el tercero con miras a alcanzar un adecuado nivel de cumplimiento, siempre y cuando la naturaleza de la operación y el tipo de Tratamiento de datos involucrado lo permita. En el evento en que no sea posible establecer un plan de acción para el cumplimiento del RCPDP por parte del tercero sin exponer a la Compañía a riesgos de incumplimiento de la ley a afectar la seguridad de la información personal, la Compañía desistirá del relacionamiento jurídico con este tercero.
- e. Una vez formalizado el vínculo jurídico o contractual con el tercero, la Compañía definirá la metodología y periodicidad de la supervisión del cumplimiento del RCPDP el tiempo que dure

la vinculación o nexo jurídico o comercial con el tercero. Si durante el periodo de supervisión se evidencia que el tercero no alcanza niveles adecuados del cumplimiento del RCPDP o realiza prácticas inseguras para el adecuado Tratamiento de los Datos Personales, la Compañía deberá definir el plan de mejora respectiva o la terminación del vínculo con el tercero según proceda en los términos expuestos.

- f. Culminado el vínculo jurídico o comercial con el tercero, el área responsable junto con la Oficina de Protección de Datos Personales procederá a solicitar la eliminación o devolución de la información personal que aún pueda conservar el tercero, tomando en consideración el principio de necesidad, vigencia y legalidad del dato.

8. POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES OCÉANOS S.A.

Para la realización de la Política de protección de datos personales, se revisó el contexto de la organización, se identificaron los grupos de Titulares de datos personales de los cuales se realiza tratamiento, se definieron los canales de atención para las consultas y reclamos, se estableció el procedimiento para consultas, la fecha de vigencia de las bases de datos y de la mencionada política.

En la Política de protección de datos personales, se incluyeron los puntos de obligatorio cumplimiento estipulados en el artículo 13 del decreto 1377 de 2013 y se tomaron como base, las cartillas publicadas en la página de la Superintendencia de Industria y Comercio (SIC).

A continuación, se describe el contenido de la Política de tratamiento de datos personales de Océanos S.A.

Para el desarrollo de sus actividades agroindustriales en territorio colombiano, OCÉANOS S.A. (en adelante "OCÉANOS" o la "Compañía"), desarrolla su actividad en las siguientes plataformas de negocio:

- *Cultivo, producción y comercialización de camarones.*

En virtud de ello, OCÉANOS ha establecido la presente POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES (en adelante "LA POLÍTICA"), la cual, contiene, a nivel general, los derechos que le asisten a los titulares de los datos privados, el tratamiento que se le da a sus datos y los mecanismos para hacer valer sus Derechos, de conformidad con la normatividad vigente, en los siguientes términos.

1. AMBITO DE APLICACIÓN

Los principios y disposiciones contenidas en La Política serán aplicables a los datos personales sobre las cuales OCÉANOS, en el territorio colombiano, desarrolle el tratamiento o sea responsable, en los términos de la Ley 1581 de 2012 y sus Decretos Reglamentarios o normas que los modifiquen o sustituyan.

Responsable de las bases de datos:

Responsable	OCÉANOS S.A.
-------------	--------------

NIT	890931654-0
Domicilio	Cartagena-Bolívar-Colombia
Dirección	Albornoz vía a Mamonal N° 1-504
Teléfono	(5) 6778400
Correo Electrónico	protecciondedatos@oceanos.com.co
Página Web	www.oceanos.com.co

2. OBJETO DE LA POLÍTICA.

LA POLÍTICA desarrolla las obligaciones contenidas en el literal k) del artículo 17 y literal f) del artículo 18 de la Ley 1581 de 2012 y las contenidas en el Artículo 2.2.2.25.3.3 del Decreto 1074 de 2015, los cuales regulan los deberes que asisten a los responsables y encargados del tratamiento de datos personales y la atención de consultas y reclamos por parte de los Titulares de los datos, así como a lo dispuesto en la Sección Tercera del Decreto 1074 de 2015 sobre "Políticas de Tratamiento", el cual dispone que "Los responsables del tratamiento deberán desarrollar sus políticas para el tratamiento de los datos personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas".

3. MARCO LEGAL

3.1 Referente a Protección de datos personales

- Constitución Política, artículo 15.
- Ley 1581 de 2012
- Decreto Reglamentario parcial 1377 de 2013
- Decreto 886 de 2014
- Decreto 1074 de 2015
- Decreto 090 de 2018
- Título V de la Circular Única de la Superintendencia de Industria y Comercio

3.2 Normativas relacionadas con el tratamiento de datos

- Resolución 1918 de 2009 sobre Historias clínicas
- Artículo 264 del Código sustantivo de trabajo referente al "ARCHIVO DE LAS EMPRESAS"
- Ley 962 de 2005, Artículos 28 y 60 referente a la "CONSERVACIÓN DE DOCUMENTOS, ARCHIVOS, MENSAJE DE DATOS"

4. DEFINICIONES

Para efectos de dar claridad y transparencia a la lectura de la presente POLÍTICA, se utilizarán las siguientes definiciones:

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales;
- **Aviso de Privacidad:** Documento físico, electrónico o en cualquier otro formato generado por el Responsable que se pone a disposición del Titular para el tratamiento de sus datos

océanos

personales. En el Aviso de Privacidad se comunica al Titular la información relativa a la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las características del tratamiento que se pretende dar a los datos personales;

- **Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento;
- **Canal de comunicación:** Medio definido y utilizado por la organización para la atención de PQRS;
- **Dato Personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;
- **Dato Privado:** Es aquel que por su naturaleza íntima o reservada sólo es relevante para el Titular del dato;
- **Dato Semiprivado:** El dato semiprivado es aquel que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector, grupo de personas o a la sociedad en general, como el dato financiero y crediticio;
- **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;
- **Datos Sensibles:** Se trata de aquella información que afecta 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 o de derechos humanos, o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos;
- **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento;
- **Oficial de Protección de Datos:** Es el funcionario designado por OCEANOS para garantizar el cumplimiento de la presente POLÍTICA;
- **Oficina de Protección de Datos:** Es el área designada por ACEITES MANUELITA para garantizar el cumplimiento de la presente POLÍTICA;
- **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;
- **Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento;
- **Transferencia:** La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un Receptor, que a su vez es responsable del Tratamiento y se encuentra dentro o fuera del país;
- **Transmisión:** Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia, cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable;
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

5. FINALIDADES DEL TRATAMIENTO DE LOS DATOS PERSONALES

OCÉANOS realizará el Tratamiento de Datos Personales de sus empleados, empleados de sus contratistas, proveedores, clientes y de los terceros que hayan otorgado la debida Autorización. En desarrollo de los principios rectores para el tratamiento de Datos Personales contemplados en la Ley 1581 de 2012, la recolección de Datos Personales por parte de **OCÉANOS** se limitará a aquellos Datos Personales que son pertinentes y adecuados para la finalidad para la cual son recolectados o requeridos conforme a la normatividad vigente. Salvo en los casos expresamente previstos en la Ley, no se podrán recolectar Datos Personales sin autorización del Titular.

OCÉANOS tiene la obligación de mantener la confidencialidad de los Datos Personales objeto de Tratamiento y sólo podrá divulgarlos mediando autorización del Titular o por solicitud expresa de las entidades de vigilancia y control y autoridades que tengan la facultad legal de solicitarla, y permitirá en todo momento y de manera gratuita conocer, actualizar y corregir la información personal del Titular de conformidad con el artículo 8 de la Ley 1581 de 2012.

El Tratamiento de datos incluye la recolección, almacenamiento, procesamiento, administración, utilización, transferencia, transmisión y destrucción, en la forma permitida por la ley y se realiza con la siguiente finalidad específica para cada caso:

- a) **Tratamiento de datos personales y sensibles de aspirantes en procesos de selección:** Se realiza para cumplir con los procesos de vinculación de: personal, estudiantes en práctica, aprendices Sena, a cargo de OCÉANOS, tales como, pero sin limitarse a: i) EL desarrollo de procesos de selección actuales y futuros; ii) Capturar información sensible como imágenes, fotos, videos, huella dactilar a través de cámaras de video vigilancia y otros dispositivos tecnológicos, para el registro de las personas que ingresan y salen de las instalaciones de OCÉANOS, control de acceso a las oficinas, establecer medidas de seguridad a sus colaboradores y visitantes, registro y uso de casinos y demás instalaciones que así lo requieran; iii) Atención de consultas, peticiones, solicitudes, acciones y reclamos, hechas por el Titular de la información o por las personas autorizadas por este o la Ley, o por entidades del sistema general de seguridad social a los que el Titular esté o hubiere estado vinculado; iv) Realizar el control y la prevención del terrorismo y de lavado de activos, incluyendo pero sin limitarse a la consulta en listas restrictivas, y toda la información necesaria requerida de acuerdo a la normatividad aplicable; v) Realizar tratamiento de la información por parte de distintas áreas de la Compañía; vi) Transmitir o transferir la información a sus compañías vinculadas en Colombia y en el exterior cuando ello sea necesario para el desarrollo de sus operaciones; vii) Transmitir o transferir la información a un tercero (denominado Encargado o Responsable respectivamente) para realizar procesos de selección de personas, realización de encuestas, servicio tercerizado de plataformas tecnológicas y otras actividades que contribuyan con el desarrollo de la operación diaria de OCÉANOS; viii) Realizar auditorías internas o externas y; ix) En general para todos los fines necesarios para la ejecución y desarrollo del objeto social de OCÉANOS.
- b) **Tratamiento de datos personales y sensibles de empleados, ex empleados, pensionados, aprendices, practicantes, sus familiares mayores y menores de edad:** Se realiza para

cumplir con las obligaciones laborales y procesos de vinculación de personal, a cargo de OCÉANOS, tales como, pero sin limitarse a: i) El desarrollo del proceso de vinculación; ii) La celebración, ejecución y terminación del contrato de trabajo, administración del personal activo, administración de nóminas y otros pagos; iii) Procesos de nómina, afiliación, pagos y reportes al sistema general de seguridad social, cajas de compensación familiar, cooperativas de ahorro del sector solidario y entidades financieras, entidades aseguradoras, agremiaciones sindicales, pago a la DIAN de las sumas retenidas, emitir certificados de ingresos y retenciones y certificados laborales; iv) Completar y actualizar historia laboral; v) Realización de los pagos salariales y no salariales en la cuenta bancaria que señale el trabajador; vi) Cumplir las obligaciones de OCÉANOS bajo el régimen colombiano de seguridad industrial y salud ocupacional; vii) Cumplimiento de fines médicos para la atención de emergencias médicas, accidentes de trabajo o enfermedades, tramitar incapacidades, promoción de jornadas de salud y atención psicológica por parte de las EPS, llevar a cabo el proceso de control de asistencia al servicio de salud, verificación de mi estado de salud física; viii) La contratación de seguros de vida y de gastos médicos o para el otorgamiento de cualquier otra prestación de naturaleza salarial o extra-salarial que derive de la relación laboral con el Empleador, de ser el caso; ix) La notificación a familiares en caso de emergencias durante el horario de trabajo o con ocasión del desarrollo del mismo; x) Capturar información sensible como imágenes, fotos, videos, huella dactilar a través de cámaras de video vigilancia y otros dispositivos tecnológicos, para el registro de las personas que ingresan y salen de las instalaciones de OCÉANOS, control de acceso a las oficinas, establecer medidas de seguridad a sus colaboradores y visitantes, registro y uso de cascos y demás instalaciones que así lo requieran; xi) El manejo de embargos judiciales a través de nómina, administración de salarios y beneficios; xii) El ejercicio de la subordinación sobre empleados y de la potestad sancionatoria, así como para evaluaciones de los empleados; xiii) La coordinación del desarrollo profesional de los empleados, el acceso de los empleados a los recursos informáticos de OCÉANOS y la asistencia en su utilización y planificación de actividades empresariales tales como: jornadas de bienestar, beneficios ofrecidos por la compañía y representar a OCÉANOS ante una Organización o Entidad externa de naturaleza pública o privada, con fines comerciales, jurídicos, sociales, educativos o cualquier otra índole correspondientes al cargo que desempeñe dentro de la compañía; xiv) Realizar estudios de seguridad adelantados por la Compañía o por terceros; xv) Gestionar la afiliación y pago de cuotas sindicales a cargo del empleado, de ser requerido; xvi) Uso fotografías, audio y video, en las publicaciones impresas, digitales y en las redes sociales de la compañía, eventos realizados por OCÉANOS; xvii) Gestionar solicitudes de créditos; xviii) Atención de consultas, peticiones, solicitudes, acciones y reclamos, hechas por el Titular de la información o por las personas autorizadas por este o la Ley, o por entidades del sistema general de seguridad social a los que el Titular esté o hubiere estado vinculado; xix) Realizar el control y la prevención del terrorismo y de lavado de activos, incluyendo pero sin limitarse a la consulta en listas restrictivas, y toda la información necesaria requerida de acuerdo a la normatividad aplicable; xx) Realizar el tratamiento de la información por parte de distintas áreas de la Compañía; xxi) Transmitir o transferir la información a sus compañías vinculadas en Colombia y en el exterior cuando ello sea necesario para el desarrollo de sus operaciones; xxii) Transmitir o transferir la información a un tercero (denominado Encargado o Responsable respectivamente) para realizar procesos de selección de personas, realización de encuestas, capacitaciones, servicio tercerizado de plataformas tecnológicas y otras actividades que contribuyan con el desarrollo de la operación diaria de OCÉANOS; xxiii)

Realizar auditorías internas o externas; y xxiv) En general para todos los fines necesarios para la ejecución y desarrollo del objeto social de OCÉANOS.

c) **Tratamiento de datos personales de Proveedores de Bienes y Servicios:** Este tratamiento tiene como fin permitir a OCÉANOS cumplir con las obligaciones precontractuales, contractuales y pos contractuales a su cargo, tales como pero sin limitarse a: i) Registrar como proveedor en los sistemas de información de la Compañía; ii) Procesar pagos a favor del proveedor; iii) Expedir o solicitar facturas, o información relacionada con estas, certificados de retención en la fuente, paz y salvos y cualquier otro documento necesario que se deba suscribir en la relación comercial con el proveedor; iv) Contactar por cualquier medio para efectos de la prestación de los servicios o el suministro de los bienes que requiera; v) Conocer y tratar los datos de los empleados y contratistas que emplee el proveedor para la prestación de dichos servicios o suministro de dichos bienes; vi) Evaluar el cumplimiento de la prestación de los servicios o el suministro de los bienes contratados; vii) Realizar análisis estadísticos y reportes de mercadeo; viii) Realizar tratamiento de la información por parte de distintas áreas de la Compañía; ix) Transmitir o transferir la información a sus compañías vinculadas en Colombia y en el exterior cuando ello sea necesario para el desarrollo de sus operaciones; x) Transmitir o transferir la información a un tercero (denominado Encargado o Responsable respectivamente) para la realización de encuestas, servicio tercerizado de plataformas tecnológicas, participación en los eventos y actividades de las agremiaciones, y otras actividades que contribuyan con el desarrollo de la operación diaria de OCÉANOS; xi) Exigir el cumplimiento de los bienes o servicios contratados; xii) Autorizar el ingreso de subcontratistas y empleados a cargo del proveedor, a las instalaciones de la Compañía; xiii) Capturar datos personales y sensibles a través de planillas y cámaras de video vigilancia, que serán almacenados por OCÉANOS para controlar el acceso a las oficinas, plantas de producción e inmuebles de OCÉANOS y establecer medidas de seguridad para colaboradores y visitantes; xiv) Registros contables, operaciones financieras, operaciones con cooperativas del sector solidario y entidades financieras, asignación y control de elementos tecnológicos, materiales y equipos en general; xv) Gestionar la prestación médica de emergencias, de ser requerido; xvi) Realizar auditorías externas e internas; xvii) Atención de consultas, peticiones, solicitudes, acciones y reclamos, hechas por el Titular de la información o las personas autorizadas por este o la Ley; xviii) Realizar el control y la prevención del terrorismo y de lavado de activos, incluyendo pero sin limitarse a la consulta en listas restrictivas, y toda la información necesaria requerida de acuerdo a la normatividad aplicable; xix) Realizar reportes de la situación financiera y estado crediticio ante las respectivas centrales de riesgos; xx) En general para todos los fines necesarios para la ejecución y desarrollo del objeto social de OCÉANOS.

d) **Tratamiento de datos personales de Clientes:** Este tratamiento tiene como fin permitir a OCÉANOS cumplir con las obligaciones precontractuales, contractuales y pos contractuales a su cargo, tales como pero sin limitarse a: i) Registrar como cliente en los sistemas de información de la Compañía; ii) Proveer servicios y productos requeridos; procesar pedidos de los productos manufacturados por OCÉANOS; iii) Dar cumplimiento a obligaciones contractuales con el Cliente, gestionar todo tipo de contratos celebrados con OCÉANOS; iv) Expedir o solicitar facturas, o información relacionada con estas; v) Contactar por cualquier medio para efectos de la prestación de los servicios o el suministro de los bienes que el Cliente requiera; vi) Realizar tratamiento de la información por parte de distintas áreas de

la Compañía; vii) Transmitir o transferir la información a sus compañías vinculadas en Colombia y en el exterior cuando ello sea necesario para el desarrollo de sus operaciones; viii) Transmitir o transferir la información a un tercero (denominado Encargado o Responsable respectivamente) para la realización de encuestas, servicio tercerizado de plataformas tecnológicas y otras actividades que contribuyan con el desarrollo de la operación diaria de OCEANOS; ix) Enviar información sobre: Nuevos productos o servicios, ofertas relacionadas con los servicios y productos que ofrece y/o desarrolla OCEANOS y/o las compañías vinculadas, por medio de correo físico, electrónico, redes sociales, celular o dispositivo móvil, vía mensajes de texto (SMS/MMS) o cualquier otro medio; x) Permitir la participación de los Titulares en actividades de mercadeo y promocionales (incluyendo la participación en concursos, rifas y sorteos), y la realización de las mismas en redes sociales; xi) Conocer la opinión del Cliente y evaluar la calidad del servicio, evaluar el cumplimiento de la prestación de los servicios o el suministro de los bienes contratados, realizar estudios de mercado y análisis estadísticos para usos internos a través del uso de encuestas y sondeos generales; implementar esquemas de fidelización; xii) Llevar a cabo procesos de auditoría interna o externa propios de la actividad comercial que OCEANOS desarrolla; xiii) Gestionar bienes y servicios proveídos por terceros para el adecuado desarrollo de la actividad comercial de OCEANOS; xiv) Responder requerimientos legales o administrativos; xv) Registros contables, operaciones financieras, operaciones con cooperativas del sector solidario y entidades financieras, asignación y control de elementos tecnológicos, materiales y equipos en general; xvi) Capturar datos personales y sensibles a través de planillas y cámaras de video vigilancia, que serán almacenados por OCEANOS para controlar el acceso a las oficinas, plantas de producción e inmuebles de OCEANOS y establecer medidas de seguridad para colaboradores y visitantes; xvii) Atención de consultas, peticiones, solicitudes, acciones y reclamos, hechas por el Titular de la información o las personas autorizadas por este o la Ley; xviii) Realizar el control y la prevención del terrorismo y de lavado de activos, incluyendo pero sin limitarse a la consulta en listas restrictivas, y toda la información necesaria requerida de acuerdo a la normatividad aplicable; xix) Realizar reportes de la situación financiera y estado crediticio ante las respectivas centrales de riesgos; xx) En general para todos los fines necesarios para la ejecución y desarrollo del objeto social de OCEANOS.

e) Tratamiento de datos personales de accionistas, representantes legales, administradores:

Tiene el propósito de que OCEANOS pueda realizar el tratamiento de datos personales de los accionistas directos y administradores, para las siguientes finalidades: i) Atender requerimientos y realizar reportes a las entidades de Inspección, Vigilancia y Control; ii) cumplimiento de obligaciones contractuales a cargo de la sociedad o a su cargo; iii), así como para identificar factores de riesgo y salud financiera de la sociedad a la que está vinculado; iv) Operaciones financieras relacionadas con el pago de dividendos, honorarios, y otras relacionadas con rol; v) Auditorías externas e internas; vi) Atención de consultas, peticiones, solicitudes, acciones y reclamos, hechas por el Titular de la información o las personas autorizadas por este o la Ley; vii) Realizar el control y la prevención del terrorismo y de lavado de activos, incluyendo pero sin limitarse a la consulta en listas restrictivas, y toda la información necesaria requerida de acuerdo a la normatividad aplicable; viii) Capturar datos personales y sensibles a través de planillas y cámaras de video vigilancia, que serán almacenados por OCEANOS para controlar el acceso a las oficinas, plantas de producción e inmuebles de OCEANOS y establecer medidas de seguridad para colaboradores y visitantes;

- ix) Realizar tratamiento de la información por parte de distintas áreas de la Compañía; x) Transmitir o transferir la información a sus compañías vinculadas en Colombia y en el exterior cuando ello sea necesario para el desarrollo de sus operaciones; xi) Transmitir o transferir la información a un tercero (denominado Encargado o Responsable respectivamente) para la realización de encuestas, servicio tercerizado de plataformas tecnológicas y otras actividades que contribuyan con el desarrollo de la operación diaria de OCÉANOS; xii) Gestionar toda la información necesaria para el cumplimiento de las obligaciones corporativas, comerciales, tributarias y contables de la Compañía; y xiii) En general para todos los fines necesarios para la ejecución y desarrollo del objeto social de esta sociedad.
- f) **Tratamiento de datos personales y sensibles de la Comunidad:** Este tratamiento tiene como fin permitir a OCÉANOS cumplir con las siguientes actividades, pero sin limitarse a ellas: i) La realización de encuestas sociodemográficas con el fin de verificar el impacto generado por la actividad socioeconómica de la Compañía y el impacto de la generación de empleos en las comunidades de influencia y contactar los líderes de las comunidades para lograr un trabajo cooperativo; Ser beneficiario de los programas de bienestar social ofrecidos a la comunidad, tales como, pero sin limitarse a éstos: Subsidio de vivienda, subsidio educativo, brigadas de salud, plan semilla; actividades recreativas, celebración de fiestas especiales, donaciones; iii) Participación en las jornadas de afiliación al Sisbén, con el fin de que las personas de la comunidad (no colaboradores), puedan acceder al régimen subsidiado y reciban los beneficios del programa de salud ofrecido por el Gobierno; iv) Transmitir o transferir la información a un tercero (denominado Encargado o Responsable respectivamente) para la realización de encuestas, servicio tercerizado de plataformas tecnológicas, atender situaciones como consecuencia de los posibles impactos de la operación de la Compañía, y otras actividades que contribuyan con el desarrollo de la operación diaria de OCÉANOS; v) Realizar auditorías internas o externas; vi) Atención de consultas, peticiones, solicitudes, acciones y reclamos, hechas por el Titular de la información o por las personas autorizadas por este o la Ley, o por entidades del sistema general de seguridad social a los que el Titular esté o hubiere estado vinculado; y vii) En general para todos los fines necesarios para la ejecución y desarrollo del objeto social de OCÉANOS.
- g) **Tratamiento de datos personales de terceros:** Este tratamiento tiene como fin permitir a OCÉANOS cumplir con las siguientes actividades, pero sin limitarse a ellas: i) Enviar información sobre ofertas, cambios en las condiciones relacionados con los servicios y productos ofrecidos por OCÉANOS, el grupo Océanos y sus compañías vinculadas; ii) Permitir la participación de los titulares en actividades de mercadeo y promocionales y la realización de las mismas en redes sociales; iii) Evaluar la calidad del servicio, realizar estudios de mercado sobre hábitos de consumo y análisis estadísticos para usos internos y realizar programas de fidelización; iv) Llevar a cabo procesos de auditoría interna o externa propios de la actividad que OCÉANOS desarrolla; v) Capturar datos personales y sensibles a través de planillas y cámaras de video vigilancia, que serán almacenados por OCÉANOS para controlar el acceso a las oficinas, plantas de producción e inmuebles de OCÉANOS y establecer medidas de seguridad para colaboradores y visitantes; vi) Incluir y almacenar una copia física o digital de documento de identificación personal o documentos que contengan información de salud y/o edad en las bases de datos de OCÉANOS para atender emergencias de salud del Titular, cuando sea necesario; vii) Realizar el control y la prevención del

terrorismo y de lavado de activos, incluyendo pero sin limitarse a la consulta en listas restrictivas, y toda la información necesaria requerida de acuerdo a la normatividad aplicable; viii) Atención de eventuales emergencias; xix) Dar respuesta a consultas, peticiones, quejas y reclamos que sean realizadas por los titulares y a organismos de control y demás autoridades que en virtud de la ley aplicable deban recibir los Datos Personales; x) Transferir la información recolectada a distintas áreas de OCEANOS y a el Grupo Océanos y sus compañías vinculadas en Colombia y en el exterior cuando ello sea necesario para el desarrollo de sus operaciones; xi) Uso de datos personales y sensibles como imagen, audio y video en publicaciones físicas, digitales, incluyendo redes sociales y página web de OCEANOS, el grupo Océanos y sus empresas vinculadas; xii) Transmitir o transferir mis datos personales a proveedores de servicios y aliados comerciales de OCEANOS, en la medida en que sea necesario para las finalidades arriba indicadas; xiii) Atención de consultas, peticiones, solicitudes, acciones y reclamos, hechas por el Titular de la información o las personas autorizadas por este o la Ley; y xiv) En general para todos los fines necesarios para la ejecución y desarrollo del objeto social de OCEANOS.

h) Parágrafo primero: Tratamiento de datos de los niños, niñas y adolescentes: OCEANOS realizará excepcionalmente el tratamiento de datos personales y sensibles de niños, niñas y adolescentes, siempre y cuando su tratamiento sea necesario para garantizar el respeto del interés superior de los niños, niñas y adolescentes, o asegurar el respeto de sus derechos fundamentales, previa autorización de Padre o Acudiente del menor, como en los siguientes eventos:

- i. Afiliación de los hijos de los colaboradores a entidades de salud, cajas de compensación.
- ii. Inclusión de los hijos de los colaboradores en las pólizas de seguro que ofrece la compañía por convenio.
- iii. Inscripción de niños, niñas y adolescentes que sean hijos de colaboradores y de personas de la comunidad, en programas educativos y de bienestar.

El tratamiento de los datos se realizará cumpliendo con lo establecido en la Ley 1581 de 2012 y el Decreto 1377 de 2013.

Para casos excepcionales donde se deba cumplir con disposiciones del gobierno nacional, situaciones que afecten la seguridad nacional y/o departamental, emergencia sanitaria, eventos donde se pueda ver afectada la integridad física de las persona, o similares, la Compañía podrá realizar el tratamiento de los siguientes datos, en aras de garantizar la seguridad de colaboradores, contratistas, personal de aseo, seguridad y en general las personas que ingresan a las instalaciones para ejercer sus labores: datos de identificación, contacto, ubicación, estado de salud, medio de movilización, afiliación a entidades de salud para cumplir con las finalidades, pero sin limitarse: Prevención, asistencia médica, monitoreo del estado de salud de las personas, informar a las Entidades de salud de pública, Policía Nacional, gestionar permisos de movilidad, contactar con red hospitalaria

6. RESPONSABILIDADES DE LA COMPAÑÍA COMO ENCARGADOS DE LOS DATOS PERSONALES

océanos

Para el tratamiento de los datos personales de los Titulares, cuando la Compañía ejerce el rol de Encargado, OCÉANOS realizará el tratamiento de los datos personales conforme a lo establecido en el artículo 18 de la Ley 1581 de 2012 (Deberes de los Encargados) y los compromisos adquiridos en los respectivos contratos de encargo.

7. DERECHOS DE LOS TITULARES

Son Derechos de los titulares de la información:

- a) Conocer, actualizar y rectificar sus datos personales frente a **OCÉANOS** o los Encargados del Tratamiento de Datos designados por esta. Este derecho se podrá ejercer, entre otros, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.
- b) Solicitar prueba de la autorización otorgada a **OCÉANOS**, salvo cuando expresamente se exceptúe como requisito para el Tratamiento.
- c) Ser informado por **OCÉANOS** como responsable del tratamiento, previa solicitud, respecto del uso que les ha dado a sus datos personales.
- d) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.
- e) Acceder en forma gratuita y de manera fácil y sencilla a sus datos personales que hayan sido objeto de Tratamiento, de acuerdo con el artículo 21 del Decreto 1377 del 2013.
- f) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a la Ley.
- g) Conocer la dependencia o persona facultada por **OCÉANOS** frente a quien podrá presentar quejas, consultas, reclamos y cualquier otra solicitud sobre sus Datos Personales.
- h) Las demás que señale la normatividad vigente.

8. RESPONSABLE Y CANALES PARA LA ATENCIÓN DE PQR DE LOS TITULARES

OCÉANOS designó como responsable de la recepción, atención y respuesta a las peticiones, quejas, reclamos y en general de cualquier tipo de consulta relacionada con los datos personales de los Titulares, al área o dependencia que se relaciona a continuación:

Empresa	OCÉANOS S.A.
Responsable atención PQRS	Departamento Jurídico

De igual forma, **OCÉANOS** ha dispuesto los siguientes canales de atención para que el titular de los datos pueda ejercer sus derechos de conocer, actualizar, rectificar, suprimir el dato, solicitar prueba de la autorización y revocar la autorización; el titular puede realizar la solicitud escrita a través de cualquiera de los siguientes mecanismos de atención al usuario, dispuesto por **OCÉANOS** a nivel nacional:

Correo electrónico:	protecciondedatos@oceanos.com.co
Oficina física:	Albornoz vía a Mamonal N° 1-504, Cartagena-Bolívar-Colombia
Página web:	www.oceanos.com.co/contacto

Horarios de atención: Días hábiles de lunes a viernes de 8:00 am a 12:00 pm y de 2:00 pm a 5:00 pm.

océanos
V.B.
DATOS JURÍDICOS

9. PROCEDIMIENTOS DE ACCESO, CONSULTA, RECTIFICACIÓN Y ACTUALIZACIÓN DE INFORMACIÓN

El Titular tiene derecho a presentar ante OCÉANOS, la solicitud (escrita) de consultas y/o reclamos, previa validación de su identidad, a través de cualquiera de los siguientes canales, de atención al usuario dispuesto a nivel nacional:

Correo electrónico:	protecciondedatos@oceanos.com.co
Oficina física:	Albornoz vía a Mamonal N° 1-504, Cartagena-Bolívar-Colombia
Página web:	www.oceanos.com.co/contacto

Horarios de atención: Días hábiles de lunes a viernes de 8:00 am a 12:00 pm y de 2:00 pm a 5:00 pm.

OCÉANOS responderá la consulta y/o reclamo por el mismo medio que fue formulado.

Consultas.

El Titular o causahabiente podrá consultar la información que reposa en las bases de datos de **OCÉANOS**, de forma gratuita, al menos una vez cada mes calendario o cuando existan modificaciones sustanciales en la Política de tratamiento de datos personales, que motiven nuevas consultas. Para esto deberá presentar la respectiva solicitud a través de los canales establecidos por **OCÉANOS** en el punto anterior, la cual deberá contener datos de identificación (Nombre, apellido, número de identificación) y así tramitar la consulta. Una vez recibida la consulta, **OCÉANOS** deberá resolverla en un término de diez (10) días hábiles contados a partir de la fecha que se recibió la misma. Cuando no fuere posible cumplir con este tiempo, se deberá informar al interesado expresando los motivos del retardo y la fecha en que se atenderá la consulta en un término no mayor a cinco (5) días.

Reclamos.

El Titular que considere que la información contenida en una base de datos de **OCÉANOS**, debe ser objeto de corrección, actualización o supresión, o cuando advierta el presunto incumplimiento de cualquiera de los deberes contenidos en la ley 1581 de 2012 o en la presente Política, podrá presentar un reclamo a **OCÉANOS**, el cual será tramitado bajo las siguientes condiciones:

1. Si el reclamo resulta incompleto, **OCÉANOS** requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del mismo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.
En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término no mayor a dos (2) días hábiles e informará de la situación al titular de la información.
2. Una vez recibido el reclamo completo, se incluirá en la base de datos correspondiente una leyenda que diga "reclamo en trámite" y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.
3. El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

Procedimiento para el uso de los canales de comunicación.

1. Si la solicitud se realiza a través de correo electrónico:
 - a. Indicar en el asunto: Consulta o Reclamo de Habeas Data
 - b. El contenido deberá tener la siguiente información:
 - i. Nombre y apellido del Titular de los datos
 - ii. Número de identificación
 - iii. La descripción de los hechos que dan lugar al reclamo
 - iv. La dirección de envío de correspondencia
 - v. Aportar los documentos que considere relevantes o soporten la solicitud.
2. Si la solicitud se realiza a través de nuestra oficina física – centro de recepción de facturación:
 - a. Puede diligenciar el formato propuesto por **OCÉANOS**
 - b. Puede traer su solicitud escrita, la cual deberá contener la siguiente información:
 - i. Indicar en el asunto: Consulta o Reclamo de Habeas Data
 - ii. Nombre y apellido del Titular de los datos
 - iii. Número de identificación
 - iv. La descripción de los hechos que dan lugar al reclamo
 - v. La dirección de envío de correspondencia
 - vi. Aportar los documentos que considere relevantes o soporten la solicitud.
3. Si la solicitud se realiza a través de la página web:
 - a. Utilizar la opción: Contacto.
 - b. Diligenciar los campos marcados como obligatorios
 - c. Número de identificación
 - d. La descripción de los hechos que dan lugar al reclamo
 - e. La dirección de envío de correspondencia
 - f. Presentar pruebas que considere relevantes o soporten la solicitud.

10. TRANSMISIONES INTERNACIONALES Y NACIONALES DE DATOS A ENCARGADOS

Cuando **OCÉANOS** requiera enviar o transmitir datos a uno o varios Encargados ubicados dentro fuera del territorio de la República de Colombia, deberá establecer cláusulas contractuales o celebrar un contrato de transmisión de Datos Personales en el que, entre otros, se pacte lo siguiente:

1. Los alcances y finalidades del Tratamiento.
2. Las actividades que el Encargado realizará en nombre de **OCÉANOS**.
3. Las obligaciones que debe cumplir el Encargado respecto del Titular del dato y **OCÉANOS**.
4. El deber del Encargado de tratar los datos de acuerdo con la finalidad autorizada para el mismo y observando los principios establecidos en la Ley colombiana y la presente POLÍTICA.
5. La obligación del Encargado de proteger adecuadamente los Datos Personales y las bases de datos, así como de guardar confidencialidad respecto del Tratamiento de los datos transmitidos.
6. Una descripción de las medidas de seguridad concretas que van a ser adoptadas tanto por **OCÉANOS** como por el Encargado de los datos en su lugar de destino.

OCÉANOS no solicitará la Autorización de transmisiones internacionales de Datos Personales cuando esta transmisión se encuentre amparada en alguna de las excepciones previstas en la Ley y sus Decretos Reglamentarios.

11. SEGURIDAD DE LA INFORMACIÓN

En desarrollo del principio de seguridad establecido en la Ley 1581 de 2012, **OCÉANOS** ha adoptado las medidas técnicas, humanas y administrativas consideradas necesarias para otorgar seguridad a los Datos Personales objeto de Tratamiento, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

12. PUBLICACIÓN Y VIGENCIA

LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES DE OCÉANOS se publicará en la página web www.oceanos.com.co. Así mismo, el presente documento constituye una modificación a las políticas de tratamiento de datos preexistentes y rige a partir del 31 de enero de 2019, y hasta el momento en que expresamente se revoque o modifique.

Las bases de datos en poder de **OCÉANOS** en las que se registran datos personales tendrán una vigencia igual al tiempo en que se mantenga y utilice la información para las finalidades descritas en esta política y se conservarán mientras no se solicite su supresión por el interesado y siempre que no exista un deber legal o contractual de conservar la información.

13. REVISIONES Y ACTUALIZACIONES

OCÉANOS se reserva el derecho de modificar los términos y condiciones del presente documento "Política de Tratamiento de Datos Personales" como parte de nuestro esfuerzo por cumplir con las obligaciones establecidas por la Ley 1581 de 2012, los decretos, reglamentarios y demás normas que complementen, modifiquen o deroguen lo contenido en este documento, con el fin de reflejar cualquier cambio en nuestras operaciones, funciones o finalidades. En los casos que esto ocurra se publicará con 15 días de anticipación a su vigencia el nuevo documento de "Política de Tratamiento de Datos Personales" en la página web: www.oceanos.com.co.

LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES de la COMPAÑÍA será revisada de manera anual o antes si es requerido y se realizarán las actualizaciones necesarias. Tanto las revisiones como las actualizaciones serán consignadas en la siguiente tabla:

Versión	Fecha	Cambios Introducidos / Revisiones
1.0	Julio / 2017	Creación de documento
2.0	Enero / 2019	Actualización de la política
2.1	Abril / 2020	Adición de portada, tabla de contenido y capítulo 13. Revisiones y actualizaciones. Tratamiento de datos para casos excepcionales Deberes como Encargados de tratamiento de datos personales

9. PROCEDIMIENTO DE ATENCIÓN DE CONSULTAS Y RECLAMOS POR PARTE DE LOS TITULARES

La Compañía elaboró el procedimiento para la atención de consultas y reclamos, llamado: Procedimiento de ejercicio de derechos, en el cual se establece los siguientes puntos: Objetivo, alcance, cubrimiento, derecho de los titulares, tiempos de respuesta, responsabilidades tanto de la Oficina de protección de datos personales, como las responsabilidades de los colaboradores que realizan tratamiento de los datos, procedimiento para atender las consultas y reclamos, formatos, y canales de atención.

1. OBJETIVO

Determinar los mecanismos, procedimientos, instancias y actividades aplicables para la atención de Consultas y Reclamos realizados por los Titulares ante el área encargada de la Protección de Datos Personales de la Compañía en el ejercicio del derecho fundamental de hábeas data.

2. ALCANCE

Este procedimiento abarca todas las actuaciones que se deben adelantar con ocasión de las Consultas y Reclamaciones que se presenten ante la Compañía en relación con el Tratamiento de Datos Personales realizado al interior de la misma.

3. DERECHOS DE LOS TITULARES

Los derechos que le asisten a los titulares ya se encuentran enunciados dentro de este documento en el apartado 8. POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES OCÉANOS S.A., sección 7. Derechos de los titulares.

Para atender las consultas o reclamaciones, se precisa lo siguiente:

Referente a la Rectificación y actualización de los datos personales

- En las solicitudes de rectificación y actualización de datos personales, el Titular debe indicar las correcciones a realizar y aportar la documentación que avale su petición.
- OCÉANOS tiene plena libertad de habilitar mecanismos que le faciliten el ejercicio de este derecho, siempre y cuando beneficien al Titular de los Datos Personales. En consecuencia, se podrán habilitar medios electrónicos u otros que la Compañía considere pertinentes y seguros.
- OCÉANOS podrá establecer formularios, formatos, sistemas y otros métodos, que serán informados en el Aviso de Privacidad y la Política de Tratamiento y que se pondrán a disposición de los interesados en la página web u oficinas de la Compañía.

Referente a la supresión de los datos personales

- En todo caso, la supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que el Responsable o Encargado ha incurrido en conductas contrarias al RCPDP y, en particular:
 - Que los mismos no estén siendo tratados conforme a los principios, deberes y obligaciones previstas en el RCPDP.

- Que hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recabados.
- Que se haya superado el periodo necesario para el cumplimiento de los fines para los que fueron recogidos.

Esta supresión implica la eliminación o borrado seguro, total o parcial, de la información personal de acuerdo con lo solicitado por el titular en los registros, archivos, bases de datos o tratamientos realizados por OCÉANOS.

El derecho de supresión no es un derecho absoluto. OCÉANOS, como Responsable del Tratamiento, puede negar o limitar el ejercicio del mismo cuando:

- El Titular tenga el deber legal o contractual de permanecer en la Base de Datos.
- La eliminación obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas.
- Los Datos Personales sean necesarios para proteger los intereses jurídicamente tutelados del Titular; para realizar una acción en función del interés público, o para cumplir con una obligación legalmente adquirida por el Titular.
- Los datos sean datos de naturaleza pública.

Referente a la revocatoria de la autorización para el tratamiento de los datos personales

- En los casos que sea posible la revocatoria de la Autorización, la misma podrá tener efecto sobre la totalidad de finalidades consentidas, o sobre algunas de ellas. En este caso, OCÉANOS deberá suspender parcialmente el Tratamiento de los Datos Personales para las finalidades indicadas por el Titular y continuar el Tratamiento respecto de las finalidades remanentes.

El derecho de revocatoria no es un derecho absoluto. OCÉANOS, como Responsable del Tratamiento de Datos Personales, puede negar o limitar el ejercicio del mismo cuando:

- El Titular de los datos tenga el deber legal o contractual de permanecer en la Base de Datos.
- La revocatoria de la Autorización del tratamiento obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas.
- Los datos sean necesarios para proteger los intereses jurídicamente tutelados del Titular; para realizar una acción en función del interés público, o para cumplir con una obligación legalmente adquirida por el titular.
- Los datos sean de naturaleza pública.

4. TIEMPOS DE RESPUESTA

Los tiempos establecidos por la Ley 1581 para dar respuesta a la solicitud o reclamo realizado por el Titular de los datos o su representante son:

- Consultas: Diez (10) días hábiles contados a partir de la fecha en que fue recibida la Consulta. Si no es posible atender la consulta en este tiempo, se informará al Titular de los datos o su representante los motivos de la demora y se dispondrá de un tiempo no mayor a cinco (5) días hábiles siguientes al vencimiento del primer término.
- Reclamos: Quince (15) días hábiles contados a partir del día siguiente a la fecha en que fue recibido el reclamo. Si no se puede dar trámite en este tiempo, se informará al Titular de los datos o su representante los motivos de la demora y se dispondrá de un tiempo no mayor a ocho (8) días hábiles siguientes al vencimiento del primer término.
- Si el reclamo resulta incompleto, OCÉANOS requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del mismo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.
- En caso de que quién reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término no mayor a dos (2) días hábiles e informará de la situación al titular de la información.

5. CANALES DE ATENCIÓN PARA LA RECEPCIÓN DE LA CONSULTA O RECLAMO

Los responsables y canales de atención habilitados por Aceites Manuelita para la recepción de consultas o reclamos pueden ser consultada dentro del presente documento en el apartado 8. POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES OCÉANOS S.A., sección 8. Responsables y canales para la atención de PQS de los titulares.

6. PROCEDIMIENTO PARA EL USO DE LOS CANALES DE ATENCIÓN POR PARTE DEL TITULAR DE LOS DATOS O SU REPRESENTANTE

El procedimiento que deben de seguir los titulares para presentar solicitudes o reclamos por medio de los canales de atención habilitados por Aceites Manuelita esta descrito dentro del presente documento en el apartado 8. POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES OCÉANOS S.A., sección 9. Procedimiento de acceso, consulta, rectificación y actualización de información.

7. FORMATOS PARA LA RECEPCIÓN DE PQRS DE HABEAS DATA

La Compañía ha dispuesto un formato físico para la recepción de consultas o reclamos de habeas data, con el fin de que el Titular de los datos o su representante los puedan utilizar cuando se acerque a las oficinas para radicar su solicitud.

- **FORMATO FÍSICO**

El formato tiene la siguiente forma:

FORMATO DE PREGUNTAS, QUEJAS, RECLAMOS Y SOLICITUDES SOBRE DATOS PERSONALES

Fecha:		
Nombre y apellido:		
Identificación:	Ciudad:	
CALIDAD EN LA QUE OBRA	DOCUMENTACION ADJUNTA	
Titular <input type="checkbox"/>	Documento de identificación <input type="checkbox"/>	
Causahabiente <input type="checkbox"/>	Registro civil y documento de identificación <input type="checkbox"/>	
Representante legal en caso de menores <input type="checkbox"/>	Padres de Familia: <input type="checkbox"/> Registro civil de nacimiento y documento de identidad.	
	Tutores: <input type="checkbox"/> Sentencia judicial que confiere representación legal.	
Representante legal autorizado por el titular <input type="checkbox"/>	Poder autenticado <input type="checkbox"/>	
Por estipulación a favor de otro <input type="checkbox"/>	Manifestación en ese sentido <input type="checkbox"/>	
Documentación de soporte para la reclamación:		
A través del presente documento realizo la siguiente consulta o reclamo de conformidad a lo establecido en la Ley Estatutaria 1581 de 2012, sus decretos reglamentarios y en la Política de protección de datos de la Compañía		
TIPO DE SOLICITUD		
(Marque con X en la casilla vacía, el tipo de solicitud que desea realizar)		
<input type="checkbox"/>	Conocer la información que se tiene o cerca de mis datos personales y el uso que dan a los mismos	
<input type="checkbox"/>	Actualizar mis datos personales	
<input type="checkbox"/>	Rectificar mis datos personales.	
<input type="checkbox"/>	Solicitar prueba de la autorización otorgada para el tratamiento de mis datos personales.	
<input type="checkbox"/>	Solicitar la supresión de mis datos personales.	
<input type="checkbox"/>	Solicitar la revocación de la autorización de tratamiento de mis datos personales.	
DATOS PERSONALES MOTIVO DE CONSULTA O RECLAMO		
(Escriba los datos personales sobre los cuales desea realizar la consulta o reclamo)		
DESCRIPCION DE LA CONSULTA O RECLAMO		
(Describa los hechos sobre los cuales se fundamenta la reclamación)		
DATOS DE CONTACTO Y RESPUESTA		
Dirección residencia:	Ciudad y Departamento:	
Teléfono (fijo o celular):	Correo electrónico:	
Firma:	Cédula:	
La consulta (Acceso) será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Para mayor información sobre los tiempos de respuesta, Por favor consultar la política de protección de datos personales publicada en la página web www.manuelita.com		
ESPACIO EXCLUSIVO PARA DILIGENCIAR POR LA COMPAÑIA		
Fecha máxima para respuesta inicial (máximo 10 días hábiles después de recibir consulta y 15 días hábiles después de recibir reclamo)	Fecha máxima para respuesta con prórroga (si se requiere) (máximo 15 días hábiles después de recibir consulta y 20 días hábiles después de recibir el reclamo)	
Persona que recibe la Consulta/Reclamo	NOMBRE	CARGO
Estado de la Solicitud	En Trámite <input type="checkbox"/>	Finalizada <input type="checkbox"/>

A continuación, se explican los campos del formato:

Fecha: DE / / AAAAA	Escriba la fecha en que se radica la consulta o reclamo, la cual debe quedar en el formato DD (día en número Ejemplo: 01), MM (mes en número, Ejemplo: 02), AAAA (año en número, Ejemplo: 2019).
Nombre y apellido:	Escriba el nombre y apellido de la persona que realiza la consulta o reclamo
Identificación:	Escriba el número de identificación de la persona que realiza la consulta o reclamo
Ciudad:	Escriba donde radica la consulta

El siguiente cuadro se divide en 2:

Calidad en la que Obra: Aquí se debe marcar con X en el recuadro una sola opción la cual identifica si la persona es el Titular o actúa en calidad de representante del mismo.

Documentación adjunta: Aquí se debe marcar con X en el recuadro la documentación que adjunta y que acredita a la persona como Titular de los datos o su representante.

Existe una relación directa entre las líneas, es decir, si la persona es el Titular, debe adjuntar Documento de Identificación y así sucesivamente como se muestra en la imagen.

Para el caso del representante legal de menores de edad solo debe adjuntar un tipo de documentación, la que le corresponda, si es Padre de familia o si es el Tutor del menor.

CALIDAD EN LA QUE OBRA	DOCUMENTACIÓN ADJUNTA
Titular <input checked="" type="checkbox"/>	Documento de identificación <input checked="" type="checkbox"/>
Causahabiente <input type="checkbox"/>	Registro civil y documento de identificación <input type="checkbox"/>
Representante legal en caso de menores <input type="checkbox"/>	Padres de Familia: <input type="checkbox"/> Registro civil de nacimiento y documento de identidad.
	Tutores: <input type="checkbox"/> Sentencia judicial que confiere representación legal.
Representante legal autorizado por el titular <input type="checkbox"/>	Poder autenticado <input type="checkbox"/>
Por estipulación a favor de otro <input type="checkbox"/>	Manifestación en ese sentido. <input type="checkbox"/>
Documentación de soporte para la reclamación: Dependiendo de la reclamación deberá adjuntar más documentación que ayude a dar trámite a su solicitud	
A través del presente documento realizo la siguiente consulta o reclamo de conformidad a lo establecido en la Ley Estatutaria 1581 de 2012, sus decretos reglamentarios y en la Política de protección de datos de la Compañía	

En el siguiente cuadro, debe marcar con X, como se indica en la imagen, el tipo de solicitud que desea realizar. Debe marcar solo una opción de las presentadas.

TIPO DE SOLICITUD	
<i>(Marque con X en la casilla vacía, el tipo de solicitud que desea realizar)</i>	
<input type="checkbox"/>	Conocer la información que se tiene a cerca de mis datos personales y el uso que dan a los mismos
<input type="checkbox"/>	Actualizar mis datos personales
<input checked="" type="checkbox"/>	Rectificar mis datos personales.
<input type="checkbox"/>	Solicitar prueba de la autorización otorgada para el tratamiento de mis datos personales.
<input type="checkbox"/>	Solicitar la supresión de mis datos personales.
<input type="checkbox"/>	Solicitar la revocación de la autorización de tratamiento de mis datos personales.

En el siguiente cuadro, la persona debe escribir el motivo de su consulta o reclamo:

DATOS PERSONALES MOTIVO DE CONSULTA O RECLAMO
<i>(Escriba los datos personales sobre los cuales desea realizar la consulta o reclamo)</i>
Espacio para escribir los datos personales sobre los cuales se está realizando la consulta o reclamo, ejemplo: Mi nombre es Pepito Pérez y en su base de datos está escrito Pepito <u>Péres</u> .

En el siguiente cuadro, la persona debe describir la consulta o reclamo:

DESCRIPCIÓN DE LA CONSULTA O RECLAMO
<i>(Describe los hechos sobre los cuales se fundamenta la reclamación)</i>
Espacio para que describa en qué se bases su consulta o reclamo. Para el ejemplo de rectificación, su reclamo se fundamenta en que su apellido no está bien escrito en la base de datos.

En el siguiente cuadro, la persona debe escribir sus datos de contacto para enviarle la respuesta a la solicitud realizada:

DATOS DE CONTACTO Y RESPUESTA	
Dirección residencia: Escriba la dirección donde desea que le llegue la respuesta a su solicitud.	Ciudad y Departamento: Escriba la ciudad Departamento a la que corresponde la dirección de residencia de la casilla anterior.
Teléfono (fijo o celular): Escriba un número de teléfono fijo o celular para contactarle	Correo electrónico: Escriba un correo electrónico (si lo tiene) donde se le pueda notificar acerca de su solicitud realizada.
Firma: Coloque su firma	Cédula: Escriba su número de identificación

En el siguiente cuadro se explica los tiempos de respuesta de la solicitud realizada:

La consulta (Acceso) será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Para mayor información sobre los tiempos de respuesta, Por favor consultar la política de protección de datos personales publicada en la página web www.manuelita.com

El siguiente cuadro es de uso exclusivo de OCEANOS ante la cual el titular de los datos o su representante realiza la solicitud. El colaborador que recibe la solicitud debe colocar su nombre y cargo. Es menester del Oficina de protección de datos diligenciar los campos de fecha máxima para respuesta inicial y respuesta máxima con prórroga. Adicionalmente deberá marcar con X el estado de la solicitud la cual al momento de recibirla estará en Trámite. Luego de la gestión y respuesta al solicitante, se deberá marcar la opción Finalizada.

ESPACIO EXCLUSIVO PARA DILIGENCIAR POR LA COMPAÑIA	
Fecha máxima para respuesta inicial (máximo 10 días hábiles después de recibir consulta y 15 días hábiles después de recibir reclamo)	Fecha máxima para respuesta con prórroga (si se requiere) (Máximo 15 días hábiles después de recibir consulta y 23 días hábiles después de recibir el reclamo)
Persona que recibe la Consulta/Reclamo	NOMBRE
	CARGO
Estado de la Solicitud	En Trámite <input type="checkbox"/> Finalizada <input type="checkbox"/>

8. GESTIÓN DE QUIEN RECIBE UNA CONSULTA O RECLAMO.

Al momento de recibir la Consulta o Reclamo, las siguientes acciones deben ser realizadas:

- Si es recibida por escrito, bien sea por correo electrónico, por la página web o en la dirección física, la Consulta o Reclamo deberá ser direccionada por parte del colaborador que la reciba, a la Oficina de Protección de Datos Personales de su Unidad de Negocio.

El tiempo máximo para que esta solicitud sea entregada al Oficina de protección de datos personales es 1 día contados a partir de la fecha de la recepción de la misma.

- Si es recibida verbalmente por vía telefónica, el colaborador que atienda la Consulta o Reclamo deberá direccionar a la persona hacia los canales establecidos, indicándole cuáles son y cómo acceder a ellos, debido a que por este medio no se puede acreditar la identidad de las personas.

9. GESTIÓN DE LA OFICINA DE PROTECCIÓN DE DATOS PERSONALES

En el momento en que la Oficina de Protección de Datos Personales recibe la consulta o reclamación para su gestión, deberá llevar a cabo las siguientes actividades:

- Radicación de la solicitud:

Independiente del canal por el que reciba la solicitud, la misma debe quedar radicada en un archivo o sistema de información que elija OCÉANOS, que sirva de control de las PQRS (peticiones, quejas, reclamos, solicitudes).

- Establecer las fechas de respuesta para la solicitud:

Una vez registrada la solicitud, se debe establecer las fechas de posibles respuestas dependiendo del tipo de trámite realizado por el solicitante, teniendo en cuenta los términos definidos en la Ley 1581.

- Revisión de la documentación entregada:

La Oficina de Protección de Datos Personales debe validar que la documentación entregada por el solicitante sea verídica, que permita identificar al solicitante, que brinde los elementos necesarios para dar trámite a la solicitud.

En el caso en el que el solicitante no brinde la información requerida o suficiente para tramitar la solicitud, se le informará lo mínimo requerido en los tiempos establecidos por en la Ley 1581.

- Trámite de la solicitud:

Identificar el tipo de trámite, el tipo de solicitud y quien o quienes son las áreas encargadas de realizar la gestión solicitada sobre los datos personales.

- Consultas:

Si el tipo de trámite es una consulta, elevar el requerimiento de la información necesaria para atender la consulta al área que corresponda y que tenga alguna relación con las razones que la motivaron (ej. El área que contactó al Titular, el área que utiliza en sus actividades los Datos del Titular, etc.), para que suministren la información requerida dentro de los dos (2) días siguientes a la elevación del requerimiento por parte de la Oficina de Protección de Datos Personales.

Una vez sea obtenida la información requerida para responder la Consulta, el proyecto de respuesta junto con todos los soportes deberá ser enviado a la Oficina de Protección de Datos Personales de OCÉANOS dentro de los cinco (5) días siguientes a la obtención de la información, para su validación y aprobación, la cual deberá ser realizada dentro de los dos (2) días siguientes a su recepción, tiempo en el cual podrá realizar cambios al proyecto de respuesta.

Una vez revisada, validada y aprobada la respuesta, ésta deberá ser enviada al Titular a más tardar al día siguiente, siempre y cuando no exceda los tiempos establecidos en la Ley 1581.

- Reclamos:

Si el tipo de trámite es una reclamación, se debe elevar el requerimiento de la información necesaria al área que corresponda y que tenga alguna relación con las razones que la motivaron (ej. El área que contactó al Titular, el área que utiliza en sus actividades los Datos del Titular, etc.), para que suministren la información requerida dentro de los tres (3) días

siguientes a la elevación del requerimiento por parte de la Oficina de Protección de Datos Personales.

Una vez sea obtenida la información requerida para responder la consulta, el proyecto de respuesta, junto con todos los soportes deberá ser enviado a la Oficina de Protección de Datos Personales dentro de los cinco (5) días siguientes a la obtención de la información, para su validación y aprobación, la cual deberá ser realizada dentro de los tres (3) días siguientes a su recepción, tiempo en el cual podrá realizar cambios al proyecto de respuesta.

Una vez revisada, validada y aprobada la respuesta, ésta deberá ser enviada al Titular dentro de los dos (2) días siguientes, siempre y cuando no exceda los tiempos establecidos en la Ley 1581.

Si no es posible dar respuesta en el término legal, se debe informar por escrito al Titular las razones que imposibilitan dar solución a su reclamación y señalar la fecha en la que será respondida su consulta, la cual no podrá superar los ocho (8) días hábiles siguientes.

10. GESTIÓN DEL ÁREA QUE SUMINISTRA LA INFORMACIÓN REQUERIDA PARA ATENDER LA CONSULTA O RECLAMO

Una vez la Oficina de Protección de Datos Personales eleva el requerimiento de la información necesaria para atender la Consulta o Reclamo, el área que suministra la información requerida para atender la Consulta o Reclamo tendrá un plazo de tres (3) días para entregar la información.

Para efectos de dar curso en término a la Consulta o Reclamo formulados por el Titular, el área encargada de suministrar la información requerida para atender la Consulta o Reclamo deberá proporcionar a la Oficina de Protección de Datos personales, como mínimo, la siguiente información:

- Origen de los Datos Personales del Titular;
- Datos Personales a disposición de OCÉANOS y sujetos a Tratamiento;
- Copia de la Autorización suscrita, de ser aplicable y en caso de encontrarse bajo la custodia del área;
- Último contacto realizado con el Titular y, de ser por escrito, copia del mismo.

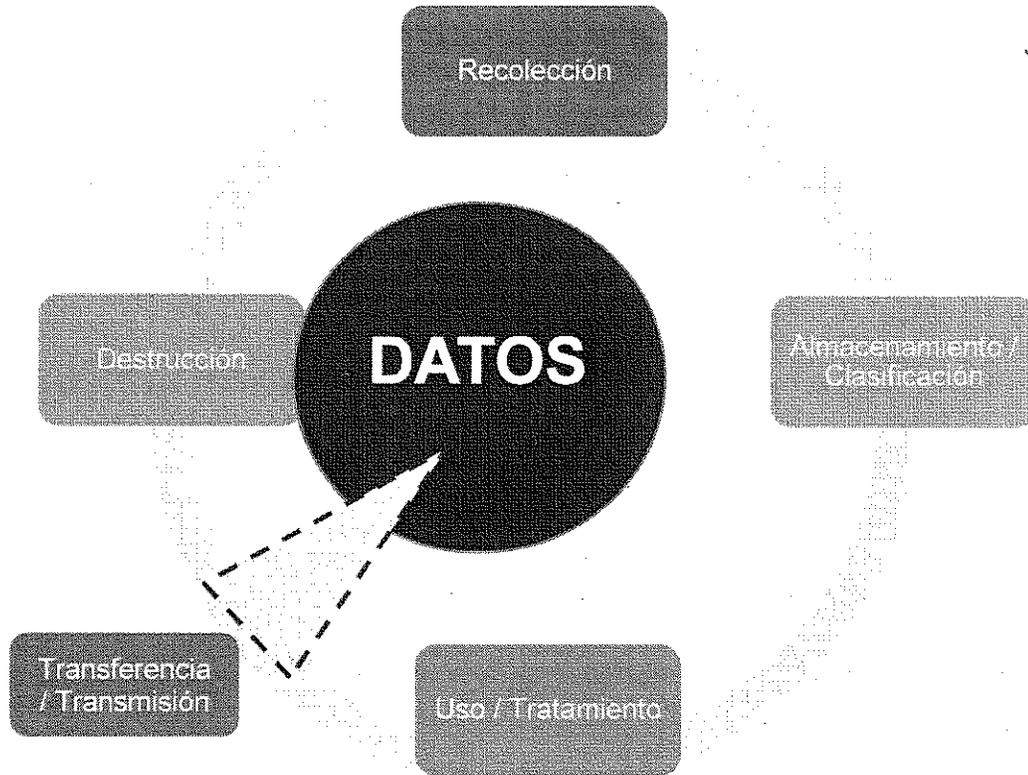
11. REFERENCIAS DOCUMENTALES

- Formato Ejercicio de derechos
- Control de solicitudes de Habeas Data

10. PROCEDIMIENTO CICLO DE VIDA DEL DATO PERSONAL

El ciclo de vida del dato personal comprende cada una de las fases de generación o recogida, conservación y utilización, comunicación o transmisión y supresión, en las cuales el dato personal es tratado

A continuación, se muestra un diagrama en el cual están definidas las fases del ciclo de vida del dato personal, empezando desde la generación y terminando en la supresión del dato personal.



Recolección: Esta primera fase tiene como objetivo identificar el origen del dato cuando ingresa a la gestión del ciclo de vida para determinar si el Responsable del tratamiento lo está recolectando de manera directa, a través de una fuente pública o a través de un tercero, que para éste último caso, se deberá contar con un contrato de transmisión o transferencia de datos personales y de la información en general. Se debe considerar además, el tipo de dato, es decir, si es público, privado, semiprivado o sensible. Desde su comienzo se especifican las finalidades de tratamiento del dato, como será tratado el dato, la manera de recolección del dato (física o digital), los medios de recolección de los datos, la solicitud de autorización de tratamiento de los datos, la seguridad de los medios recolección para garantizar la confidencialidad e integridad del dato.

Almacenamiento / Clasificación: Esta fase tiene como objetivo almacenar la información conforme se ha establecido para su tratamiento. Este punto es de vital importancia ya que se debe establecer el tiempo de conservación de la misma, es decir, se debe identificar existe alguna Ley, normativa, o política de la Compañía que establezca la razón de la recolección de los datos. Una vez determinado este punto, se debe almacenar en los medios necesarios para su tratamiento, garantizando la confidencialidad, integridad y disponibilidad de la misma.

Se debe establecer el tiempo de conservación de la información, con el fin de cumplir con lo requerido por la Ley, garantizando que la información se conservará durante el tiempo que ésta

tenga valor y utilidad para la Compañía y el que demande las Leyes que demandan su recolección y conservación.

Uso / Tratamiento: Esta fase tiene como objetivo realizar el tratamiento de los datos personales, según lo establecido en la Política de protección de datos personales de la Compañía y lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios. Se deben hacer los ajustes necesarios de manera documental y técnica para que la utilización de los datos personales sea adecuada y que se garantice la confidencialidad, integridad y disponibilidad. Por lo anterior se deben aplicar todos y cada uno de los controles establecidos en el sistema de gestión de datos personales y en el sistema de gestión de seguridad de la información.

Transmisión / Transferencia: Esta fase tiene como objetivo identificar los datos que son transferidos (Datos cedidos de un Responsable a otro Responsable de los datos personales) y cuáles son transmitidos (Datos entregados a un tercero en calidad de encargo) dentro y fuera del territorio nacional y de esta manera identificar qué tipo de controles se deben aplicar en este proceso (controles a los datos, a los encargados, a los responsables). Esta actividad se puede dar en cualquiera de las fases del ciclo de vida del dato.

Borrado / Destrucción: Se valida que cuando finaliza el tratamiento del dato según la finalidad autorizada por el titular, éste debe ser eliminado de manera segura, si no existiera una obligación legal o contractual para conservarlos. Para la eliminación del dato, se debe realizar un acta que deje constancia del proceso mismo de supresión o destrucción. Dado el caso en el que sea necesario conservar el dato, pero sin hacer tratamiento del mismo, se deberá realizar el proceso de inactivación en los sistemas de información en producción y alojarlo en el sistema de almacenamiento que se tenga implementado

La siguiente tabla actúa como una guía en el entendimiento del ciclo de vida de los datos. En la parte superior están los ciclos y en las filas se describe qué proceso actúa en determinada fase, qué datos son tratados, si se involucran terceros en este tratamiento y si se involucra tecnología. Lo anterior para poder determinar los riesgos de este tratamiento y donde se debe implementar mayores controles.

		Ciclo de vida de los datos en las operaciones del tratamiento				
		Captura de datos	Clasificación / Almacenamiento	Uso / Tratamiento	Transmisión / Transferencia	Destrucción
Elementos que intervienen en las operaciones de tratamiento	Actividades del proceso					
	Datos tratados					
	Intervinientes involucrados					
	Tecnologías interviniendo					

PASOS A SEGUIR

5.1. Recolección

No.	ACTIVIDADES	RESPONSABLE
5.1.1	Identificar cuándo se recolecta o se crea el dato personal, para determinar el origen del mismo.	Todos los procesos
5.1.2	Identificar el tipo de dato, con el fin de determinar su tratamiento y establecer los medios apropiados de almacenamiento o brindar los mecanismos de seguridad para proteger los datos	Gerencia responsable / propietario del activo / Oficina de seguridad de la información
5.1.3	Definir los medios de recolección de los datos personales y establecer la seguridad de estos medios para garantizar la confidencialidad, integridad y disponibilidad	Gerencia responsable / propietario del activo / Oficina de seguridad de la información
5.1.4	Solicitar la autorización del titular e informar la finalidad, este consentimiento debe ser expreso, informado y previo a la realización del tratamiento salvo los casos exceptuados por la Ley. Se debe dejar prueba de la autorización en cualquier medio para poderla consultar posteriormente. Si no se cuenta con la autorización del titular, el dato no podrá ser tratado y se debe continuar con el proceso de supresión.	Todos los procesos
5.1.5	Almacenar la autorización brindada por el titular.	Gerencia responsable / Propietario del activo
5.1.6	Validar que el dato sea usado para los fines establecidos y autorizados, dependiendo de los fines de la política de protección de datos personales de la Compañía, y aplicando los modelos de contratos, autorizaciones de tratamiento y avisos de privacidad definidos por esta. De no ser así, el dato no podrá ser tratado y se debe continuar con el proceso de supresión.	Gerencia responsable / Propietario del activo / Oficina de protección de datos personales
5.1.7	Evaluar la pertinencia y calidad de los datos para garantizar que son correctos y apropiados, de no ser así, tomar las medidas necesarias para lograrlo. Ejemplo: No solicitar tipo de cuenta bancaria para un registro a una capacitación. Validar la escritura de los nombres, números de cédula, etc.	Gerencia responsable / Propietario del activo

5.2. Almacenamiento / Clasificación

No.	ACTIVIDADES	RESPONSABLE
5.2.1	Clasificar los datos personales para establecer los niveles de protección adecuados.	Oficina de Protección de datos / Oficina de Seguridad de la información / Propietario del activo
5.2.2	Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. El almacenamiento de información se podrá realizar en medios digitales o físicos según sea requerido.	Oficina de Seguridad de la información / Propietario del activo
5.2.3	Establecer el tiempo de conservación de los datos, identificar si existe alguna Ley, normativa, o política de la Compañía que establezca la razón de su conservación y el tiempo del mismo	Todos los procesos
5.2.4	Implementar medidas de seguridad y políticas de acceso para garantizar la confidencialidad, disponibilidad e integridad de los mismos.	Oficina de Seguridad de la información
5.2.5	Respaldar los datos de manera periódica para garantizar la disponibilidad de los mismos.	T.I.

5.3. Uso / Tratamiento

No.	ACTIVIDADES	RESPONSABLE
5.3.1	Realizar el tratamiento del dato personal teniendo en cuenta las finalidades establecidas, comunicadas y autorizadas.	Todos los procesos
5.3.2	Durante el tratamiento de los datos personales, aplicar los controles de seguridad y privacidad, según su nivel de clasificación del dato.	Todos los procesos
5.3.3	Identificar los datos personales, personas, áreas y demás que intervienen en la transferencia y/o transmisión de información.	Oficina de Protección de datos personales / Todos los procesos
5.3.4	Realizar Contratos de encargo de tratamiento de datos personales	Oficina de Protección de datos personales
5.3.5	Validar constantemente que solamente tiene acceso a los datos personales, el personal que requiere el tratamiento acorde con sus funciones.	Líder del proceso
5.3.6	Identificar los procedimientos o actividades internas en las que se procesan datos.	Oficina de Protección de datos personales

No.	ACTIVIDADES	RESPONSABLE
		/Oficina de Seguridad de la información
5.3.7	Realizar depuración, consolidación e integración de datos.	Todos los procesos.
5.3.8	Realizar la actualización constante de los datos para garantizar la calidad de los mismos.	Todos los procesos
5.3.9	Revisar los controles de seguridad implementados y aquellos nuevos que se requieran para garantizar la seguridad de la información.	Oficina de Seguridad de la información
5.3.10	Definir y probar constantemente el procedimiento de atención de PQRS relacionadas con datos personales.	Oficina de Protección de datos personales
5.3.11	Definir un procedimiento para uso y circulación de datos personales así como para su actualización.	Oficina de Protección de datos personales
5.3.12	Notificar oportunamente los cambios en el tratamiento y la finalidad para la cual fueron obtenidos los datos personales.	Oficina de Protección de datos personales

5.4. Transmisión / Transferencia

No.	ACTIVIDADES	RESPONSABLE
5.4.1	Identificar de manera previa a la recolección del dato si éste será transmitido o transferido	Propietario del activo /Líder del proceso / Oficina de Protección de datos personales
5.4.2	Identificar los medios de transmisión o transferencia	Propietario del activo / Líder del proceso
5.4.3	Identificar el encargado o responsable de los datos personales	Líder del proceso / Oficina de Protección de datos personales
5.4.4	Generar y firmar contrato de encargo, transmisión o transferencia según aplique	Líder del proceso / Oficina de Protección de datos personales
5.4.5	Realizar auditoría para garantizar el cumplimiento de las obligaciones por parte del encargado de los datos.	Líder del proceso /Propietario del activo / Oficina de Protección de datos personales / Oficina

No.	ACTIVIDADES	RESPONSABLE
		de Seguridad de la información .

5.5. Borrado / Destrucción

No.	ACTIVIDADES	RESPONSABLE
5.5.1	Una vez finalizado el tratamiento según la finalidad autorizada por el titular o por el término establecido para su tratamiento, esta se debe eliminar de manera segura, siempre y cuando no se requiera su conservación para fines legales o contractuales.	Propietario del activo /Líder del proceso / Oficina de Protección de datos personales
5.5.2	Definir el procedimiento para atender las PQRS relacionadas con la revocación de la autorización y la supresión del dato.	Oficina de Protección de datos personales
5.5.3	Garantizar la supresión de las identidades de los titulares cuando se requiera.	Oficina de Protección de datos personales /Líder del proceso
5.5.4	Generar y almacenar reportes y constancias de la eliminación de datos personales.	Líder del proceso /Propietario del activo
5.5.5	Documentar toda la gestión de incidentes relacionada con la eliminación de los datos personales.	Líder del proceso /Propietario del activo
5.5.6	Información digital: Todas las copias y la información que la soporta debe ser eliminada de manera segura.	Líder del proceso /Propietario del activo
5.5.7	Información física: la documentación contenida en documentos, no debe ser reutilizada, esta debe ser eliminada asegurando su destrucción total.	Líder del proceso /Propietario del activo
5.5.8	Llevar a cabo la supervisión de los dispositivos que almacenan las copias de seguridad de estos datos.	T.I.
5.5.9	Controlar cualquier operación realizada sobre un dispositivo: mantenimiento, reparación, sustitución, etc.	Líder de proceso /T.I.
5.5.10	Asegurar que se cumple con la cadena de custodia cuando se trasladen los dispositivos de almacenamiento a instalaciones externas de la compañía, donde serían eliminados.	T.I.
5.5.11	Utilizar métodos de destrucción física de dispositivos electrónicos y documentación física, de acuerdo con la Política ambiental de la compañía.	Líder de proceso /T.I.

Nota: Para el proceso de eliminación, tener en cuenta el Procedimiento estándar eliminación de información de la compañía.

11. PROCEDIMIENTO DE PRIVACIDAD DESDE EL DISEÑO

OBJETIVO

Incorporar los principios de privacidad en todos los procesos de diseño, entendimiento, implementación, gestión y revisión de los sistemas, proyectos y servicios de la unidad de negocio de Océanos S.A. para garantizar la protección de los datos personales de los Titulares.

ALCANCE

Este Instructivo es aplicable a todos los procesos de Océanos S.A. que realizan el tratamiento de datos personales de Titulares.

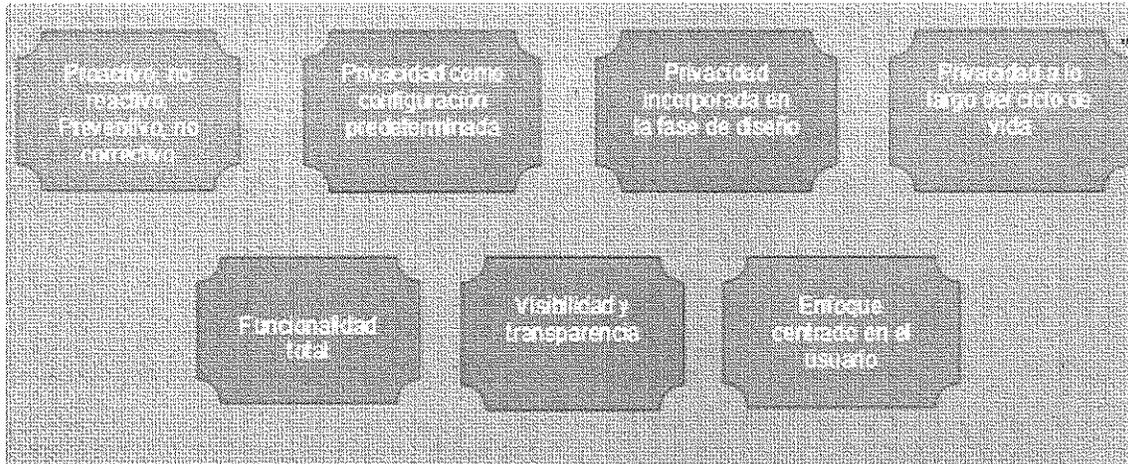
DEFINICIONES

- **Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento.
- **Ciclo de Vida del dato personal:** Comprende cada una de las fases de generación o recogida, conservación y utilización, comunicación o transmisión y supresión, en las cuales el dato personal es tratado.
- **Computación en la nube:** Tecnología que permite gestionar servicios informáticos de manera remota, de tal forma que cualquier servicio o procesamiento de datos, que antes se realizaba localmente, puede ejecutarse a través de la red de Internet, tal como el uso de aplicaciones, almacenamiento, gestión de datos, entre otros, haciendo un uso eficiente y económico de recursos al compartir hardware y software como plataformas, licencias, capacidad de almacenamiento y servicios con muchos, usuarios, con un alto nivel de disponibilidad, flexibles y por demanda.
- **Dato Personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinable.
- **Privacidad desde el diseño (Privacy by Design):** Garantizar los derechos y libertades de los interesados en lo que al tratamiento de sus datos personales se refiere y se apoya en el enfoque de riesgo, como planteamiento dinámico y de mejora continua para entender los riesgos a la privacidad y determinar las medidas técnicas y organizativas a implantar, y en la responsabilidad proactiva, entendida como un autoanálisis crítico, continuo y rastreado del responsable del tratamiento en el cumplimiento de las obligaciones que le exige la normativa, estableciendo estrategias que incorporen la protección de la privacidad a lo largo de todo el ciclo de vida del objeto (ya sea este un sistema, un producto hardware o software, un servicio o un proceso)
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

CONDICIONES GENERALES

La transformación digital que están viviendo actualmente las empresas conlleva a un crecimiento tecnológico que requiere una creación continua de sistemas, proyectos y servicios, en los cuales se realiza un constante tratamiento de datos personales. Es importante que la organización pueda garantizar el aseguramiento y privacidad de los datos personales teniendo como referencia el ciclo de vida del dato personal, desde el momento en el que se plantea su diseño hasta su despliegue e implementación.

Tomando como referencia lo anterior, se presentan los principios de privacidad desde el diseño aplicables a la organización:



- 1. Proactivo, no reactivo; Preventivo, no correctivo**
La privacidad desde el diseño debe anticiparse a los eventos o incidentes que puedan afectar los datos personales de los titulares antes de que estos sucedan.
- 2. La privacidad como configuración predeterminada**
Se debe brindar a los titulares el máximo nivel de privacidad y seguridad de sus datos personales minimizando la cantidad de datos tratados durante el ciclo de vida del dato personal.
- 3. Privacidad incorporada en la fase de diseño**
La privacidad debe ser concebida como parte imperativa en el diseño de sistemas, proyectos y servicios, así como de las prácticas de negocio y procesos de la organización para evitar subsanar errores cuando ya estos se encuentran implementados o en producción.
- 4. Funcionalidad total: pensamiento "todos ganan"**
Se debe encontrar el balance entre privacidad, usabilidad, beneficio empresarial y seguridad, garantizando que se gestionen de manera correcta los riesgos de privacidad.
- 5. Aseguramiento de la privacidad en todo el ciclo de vida.**
Se debe garantizar la privacidad en todas las etapas del ciclo de vida del dato personal (Recolección, Almacenamiento/Clasificación, uso/tratamiento, transferencia/transmisión y destrucción) y establecer medidas que propendan a la confidencialidad, integridad y disponibilidad de los sistemas, proyectos y servicios.
- 6. Visibilidad y transparencia**
Se debe indicar de manera clara, toda y cada una las finalidades del tratamiento a los que serán sometidos los datos de los titulares, así como los derechos que le asisten cómo titular y los canales de atención definidos para tal fin.

7. Enfoque centrado en el sujeto de los datos

Se debe tener respeto por la privacidad de los datos de los titulares garantizando que se definan ajustes de privacidad por defecto, diseñando procesos, aplicaciones, productos y servicios teniendo al usuario en mente y anticipándose a sus necesidades. El titular debe tener un papel activo en la gestión de sus propios datos y en el control de la gestión que otros hagan con ellos.

DESCRIPCIÓN

A continuación, se presentan las actividades generales para la implementación desde el diseño nuevos sistemas, proyectos y servicios.

Actividades desde el diseño para sistemas, proyectos y servicios

No.	Actividad	Principios asociados	Responsable	Salida
1	Realizar un análisis de riesgos de protección de datos desde la fase de diseño para los nuevos sistemas, proyectos o servicios a implementar en la organización, que involucren datos personales.	1. Proactivo, no reactivo; Preventivo, no correctivo 3. Privacidad incorporada en la fase de diseño	Oficina de protección de datos personales, Oficina de seguridad de la información, Área responsable del proyecto/ Líder del proyecto	Matriz de riesgos Acta de reunión
3	Formalizar por medio de acta los planes de tratamiento de riesgos y actividades definidas para el proyecto, servicio o sistema, donde se involucren datos personales.	5. Aseguramiento de la privacidad en todo el ciclo de vida.	Oficina de protección de datos personales y Oficina de Seguridad de la información	Matriz de riesgos Acta con planes de tratamiento de riesgos
4	Definir la cantidad mínima necesaria de datos que permitan el correcto funcionamiento del sistema, proyecto o servicio.	2. La privacidad como configuración predeterminada 4. Funcionalidad total: pensamiento "todos ganan"	Área responsable del proyecto/ Líder del proyecto	Acta de reunión
5	Se deben generar los avisos de privacidad o los textos de autorización de tratamiento de datos específicos para cada	6. Visibilidad y transparencia	Oficina de protección de datos personales, Área responsable del	Avisos de privacidad

	fuentes de recolección de datos en los proyectos, servicio o sistemas diseñados.		proyecto/ Líder del proyecto	Autorizaciones de tratamiento de datos
6	Solicitar la autorización de tratamiento de datos por parte del titular indicando claramente la finalidad o finalidades para las cuales se tratarán los datos de manera previa, expresa e informada	2. La privacidad como configuración predeterminada	Área responsable del proyecto	Autorizaciones de tratamiento de datos Firmados
7	Validar el tratamiento realizado a los datos personales del proyecto, sistema o servicios en cada una de las fases, según lo definido en el procedimiento de ciclo de vida del dato personal.	5. Aseguramiento de la privacidad en todo el ciclo de vida.	Oficina de protección de datos personales, Área responsable del proyecto/ Líder del proyecto	Acta de seguimiento del proyecto
8	En los proyectos que involucren infraestructura tecnológica, se debe tener en cuenta la privacidad de los datos de los titulares desde la configuración inicial.	7. Enfoque centrado en el sujeto de los datos	Oficina de seguridad de la información, Área responsable del proyecto/ Líder del proyecto	N/A
9	Asegurarse de dar a conocer, dentro de los términos y condiciones del proyecto, los canales de atención a las solicitudes de los titulares así como como las finalidades autorizadas.	7. Enfoque centrado en el sujeto de los datos	Oficina de protección de datos personales	Texto términos y condiciones
10	Realizar seguimiento a los planes de tratamientos de riesgos y actividades de PDP definidas desde el diseño de servicios, proyectos o sistemas.	5. Aseguramiento de la privacidad en todo el ciclo de vida.	Oficina de protección de datos personales y Oficina de Seguridad de la información	Acta de seguimiento del proyecto

Para el diseño de sistemas, proyectos o servicios que requieren específicamente servicios de computación en la nube (Cloud Computing) se establecen adicionalmente las siguientes actividades.

Actividades para sistemas, proyectos o servicios que requieran Cloud Computing

No.	Actividad	Principios asociados	Responsable
1	Notificar a la oficina de seguridad de la información y la oficina de protección de datos personales los requerimientos de nuevos productos, servicios o sistemas relacionados con Cloud Computing	5. Aseguramiento de la privacidad en todo el ciclo de vida.	Área responsable del proyecto/ Líder del proyecto
2	Identificar qué tipos de datos serán objeto de tratamiento en la nube. (públicos, privados, semiprivados o sensibles)	1. Proactivo, no reactivo; Preventivo, no correctivo	Oficina de protección de datos personales, Área responsable del proyecto/ Líder del proyecto
3	Realizar un análisis de riesgos de protección de datos desde la fase de diseño para todos los nuevos sistemas, proyectos o servicios a implementar en la organización, asociados la externalización en Cloud Computing. Validar la posible falta de control de los datos y la posible falta de información sobre el tratamiento y las condiciones en las que se presta el servicio.	1. Proactivo, no reactivo; Preventivo, no correctivo 3. Privacidad incorporada en la fase de diseño	Oficina de protección de datos personales, Oficina de seguridad de la información, en conjunto con el Área responsable del proyecto/ Líder del proyecto
4	Formalizar por medio de acta los planes de tratamiento de riesgos de Cloud Computing y actividades definidas para el proyecto, servicio o sistema, relacionadas con protección de datos.	5. Aseguramiento de la privacidad en todo el ciclo de vida.	Oficina de protección de datos personales Oficina de seguridad de la información
5	Realizar análisis y validación de reputación del proveedor.	1. Proactivo, no reactivo; Preventivo, no correctivo	Área de abastecimiento, Área responsable del proyecto/ Líder del proyecto
6	Identificar la localización física de los Data Centers en los cuales se almacenará la información	1. Proactivo, no reactivo; Preventivo, no correctivo	Oficina de seguridad de la información junto con el Área responsable del proyecto/ Líder del proyecto
7	Armonización de las legislaciones de los países de los proveedores con lo establecido en Colombia.	4. Funcionalidad total: pensamiento "todos ganan"	Oficina de protección de datos personales

8	Determinar si hay cooperación transfronteriza según el país de localización física de los Data Centers.	4. Funcionalidad total: pensamiento "todos ganan"	Oficina de protección de datos personales
9	En caso de no poder generar un contrato propio, de debe conocer y entender los términos del contrato de servicios que ofrece el proveedor para validar el cumplimiento de protección de datos personales, y de ser necesario, agregar un anexo que complemente las obligaciones de las partes.	2. La privacidad como configuración predeterminada	Oficina de protección de datos personales Oficina de seguridad de la información
10	Realizar contrato de servicio y encargo de tratamiento de datos con los proveedores de servicios Cloud donde se establezcan medidas de seguridad física y lógica, así como responsabilidades en el tratamiento de datos en cada una de las fases del ciclo de vida del dato personal y atención de PQRS. Adicionalmente se debe Limitar al máximo las finalidades de tratamiento que realizará el proveedor	2. La privacidad como configuración predeterminada	Oficina de protección de datos personales Oficina de seguridad de la información
11	Realizar contrato de transmisión de datos personales en donde se comprometa al encargado a cumplir con los principios de tratamiento de datos personales, medidas técnicas de seguridad y confidencialidad sobre los datos que tenga acceso.	2. La privacidad como configuración predeterminada	Oficina de protección de datos personales Oficina de seguridad de la información
12	Definir contractualmente las auditorias de revisión para el proveedor de Cloud en materia de PDP.	6. Visibilidad y transparencia	Oficina de protección de datos personales Oficina de seguridad de la información junto con el Área responsable del proyecto/ Líder del proyecto
13	Definir los términos de la devolución o destrucción de la información entregada al proveedor, teniendo en cuenta los procedimientos de destrucción de	5. Aseguramiento de la privacidad en todo el ciclo de vida.	Oficina de protección de datos personales Oficina de seguridad de la información

	información definidos en la organización.		
14	Definir acuerdos de confidencialidad entre la organización, el proveedor y eventualmente sus subcontratistas.	2. La privacidad como configuración predeterminada	Oficina de protección de datos personales
15	Acordar SLA's del servicio y las sanciones por incumplimiento.	3. Privacidad incorporada en la fase de diseño	Oficina de seguridad de la información Área responsable del proyecto/ Líder del proyecto
16	Definir los canales y tiempos de atención de ejercicios de derechos a los que está obligado el proveedor de Cloud, los cuales deben estar alineados a lo establecido en la Ley aplicable.	7. Visibilidad y transparencia	Oficina de protección de datos personales
17	Identificar si existe subcontratación por parte del proveedor de Cloud y definir las condiciones específicas para estos.	1. Proactivo, no reactivo; Preventivo, no correctivo	Oficina de protección de datos personales Oficina de seguridad de la información
18	Identificar medidas técnicas que aseguran la confidencialidad, integridad y disponibilidad de los datos durante el tránsito desde su origen hasta el final. Estas medidas deben estar descritas en el contrato.	1. Proactivo, no reactivo; Preventivo, no correctivo	Oficina de seguridad de la información
19	Realizar capacitación y sensibilización en materia de PDP a terceros.	4. Funcionalidad total: pensamiento "todos ganan"	Oficina de protección de datos personales
20	Realizar seguimiento a los planes de tratamientos de riesgos y actividades de PDP definidas desde el diseño de servicios, proyectos o sistemas.	5. Aseguramiento de la privacidad en todo el ciclo de vida.	Oficina de protección de datos personales Oficina de seguridad de la información

SEGUIMIENTO Y CONTROL

Se deben realizar reuniones desde la fase inicial de los sistemas, proyectos o servicios, con el fin de garantizar la privacidad desde el diseño. Estas reuniones deben generar un acta en el cual se evidencie las decisiones adoptadas a nivel de privacidad, así como sus respectivos soportes.

DOCUMENTOS DE REFERENCIA

- Procedimiento del ciclo de vida del dato personal
- Guía de protección de datos personales en los servicios de computación en la nube (Cloud Computing) - SIC
- Guía Accountability - SIC

12. PROCEDIMIENTO GENERACIÓN DE REPORTES

OBJETIVO

Establecer una estructura para generar reportes a los interesados internos y externos del programa de protección de datos personales, que permita mantenerlos plenamente informados acerca del avance de las principales actividades desarrolladas en materia de privacidad, implementadas en la organización.

ALCANCE

Garantizar la generación y envío de reportes relacionados con la protección de datos personales.

CUBRIMIENTO

Este procedimiento aplica para la Unidad de negocio de Océanos S.A

GLOSARIO

TÉRMINO	DEFINICIÓN
Autorización	Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.
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.
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.
Impacto	Simulación de las consecuencias que podrían representarse si el riesgo detectado se convirtiera en realidad.

Interesados Externos	Personal externo de la organización que debe ser notificada acerca del programa de protección de datos personales.
Interesados Internos	Personal interno de la organización que trata datos personales almacenados en las bases de datos.
Reporte	Documento que pretende transmitir una información, aunque puede tener diversos objetivos.
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.
Titular	Persona natural cuyos datos personales sean objeto de tratamiento.
Tratamiento	Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

POLÍTICAS GENERALES

1. Se deben establecer mecanismos de información internos para reportar dentro de la organización acerca del seguimiento y ejecución del programa de protección de datos personales e identificar los procedimientos a seguir en caso de que se detecten riesgos en la administración de la información de los Titulares.
2. La producción del material que sustente la implementación del programa de protección de datos personales en la compañía debe incluirse dentro de la información enviada a las gerencias, procesos y representantes legales con el fin de mantenerlos plenamente informados.
3. Es importante la notificación interna del estado del programa de protección de datos personales, ya que esto ayuda a la sensibilización de todo el personal y propende por la identificación de vulnerabilidades asociadas a privacidad.

PASOS A SEGUIR

1. Dar a conocer la estructura del sistema de protección de datos personales, enviando un informe a las gerencias, procesos y representantes legales.
Responsable: Oficina de protección de datos
2. Notificar dentro del comité de PDP y SGSI el estado actual del programa de protección de datos personales, realizando la revisión continua del programa.
Responsable: Oficina de protección de datos y Oficina de Seguridad de la Información.

3. Informar a los interesados internos acerca de la documentación producida en la implementación del programa de protección de datos personales, generando el listado maestro de documentos.

Responsable: Oficina de protección de datos y Oficina de Seguridad de la Información.

4. Comunicar a los interesados internos los resultados de las auditorías internas al programa protección de datos personales.

Responsable: Auditoría Interna

5. Comunicar a los interesados internos los resultados de los monitoreos internos al programa de protección de datos personales.

Responsable: Oficina de protección de datos

6. Reportar al Oficina de Protección de datos y al Coordinador de Tecnología el seguimiento a nuevas leyes, decretos, regulaciones, entre otras de protección de datos, realizando actualización en temas jurídicos correspondientes a protección de datos personales.

Responsable: Jurídico

7. Reportar a la Gerencia General los incidentes y vulneraciones de datos personales, programando una reunión de revisión gerencial y presentar el informe de incidentes de protección de datos.

Responsable: Oficina de protección de datos.

8. Notificar a clientes, titulares, proveedores, autoridades de protección de datos y demás interesados externos cambios sustanciales en las políticas y manuales de protección de datos personales.

Responsable: Oficina de protección de datos

9. Notificaciones, actualizaciones y reportes ante la SIC a través de la página web del Registro Nacional de Bases de Datos RNBD:

9.1. Notificar incidentes y vulneraciones de datos personales

Responsable: Oficina de protección de datos.

9.2. Reportar los ejercicios de derechos realizados por parte de los titulares

Responsable: Oficina de protección de datos

9.3. Actualizar y registrar las Bases de Datos listadas por la compañía

Responsable: Oficina de protección de datos

REFERENCIAS DOCUMENTALES

- Caracterización de Protección de Datos Personales
- Página Web SIC:

<http://www.sic.gov.co/proteccion-de-datos-personales>

13. DOCUMENTOS ADICIONALES

Los siguientes documentos fueron creados como parte del programa integral de Protección de Datos Personales:

- Indicadores del sistema de gestión de protección de datos personales
- Indicadores Programa de Inducción
- Formato: Control de solicitudes de Habeas Data
- Formato Ejercicio de derechos
- Política Tratamiento Datos Personales
- Manual para la gestión de riesgos
- Matriz de cumplimiento normativo
- Matriz Gestion de riesgos PDP
- Inventario bases de datos
- AUTORIZACIÓN TRABAJADORES
- AUTORIZACIÓN ACCIONISTAS
- AUTORIZACIÓN ASPIRANTES
- AUTORIZACIÓN CLIENTES
- AUTORIZACIÓN COMUNIDAD
- AUTORIZACIÓN PROVEEDORES
- AUTORIZACIÓN TERCEROS
- Procedimiento estándar eliminación de información
- Formato acta de eliminación de información
- Reporte de incidente de seguridad de la información
- Plan de comunicación partes internas y externas – programa de PDP OCÉANOS S.A.
- Modelo acuerdo de confidencialidad proveedores
- Modelo de cláusula de confidencialidad y protección de datos personales para colaboradores
- Modelo de cláusula de tratamiento de datos personales contrato con personas jurídicas
- Modelo contrato de transmisión de datos personales
- Modelo contrato de transferencia de datos personales
- Modelos de aviso de privacidad
- Pendón tratamiento de datos