Política de tratamiento y protección de Datos personales

2019

Aprobado por (Propietario)

Firma:_____
Nombre: Juan Carlos Uribe Rodríguez
Función: Gerente

Cláusula de Confidencialidad

La presente Política incluye información que debe ser guardada y tratada de forma confidencial. Queda prohibida la reproducción, distribución, comunicación pública, transformación, total o parcial, gratuita u onerosa, por cualquier medio o procedimiento, sin la autorización previa y por escrito de OESÍA. Este documento es estrictamente confidencial. Asimismo, tampoco podrá ser objeto de préstamo, alquiler o cualquier forma de cesión de uso sin el permiso previo y escrito de OESÍA., titular del copyright. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga acceso a la documentación será perseguido conforme la ley.

Contenido

1 Introducción

El presente Documento de Política de tratamiento y Protección de Datos Personales ha sido elaborado a instancias de **Oesía.** El marco legal que regula la política de protección de datos personales se regula en las siguientes disposiciones:

- Art 15 Constitución Política de Colombia.
- Ley Estatutaria 1266 de 2008- HABEAS DATA
- Ley Estatutaria 1581 de 2012
- Decreto 1377 de 2013
- Decreto 886 de 2014- Reglamento bases de datos personales

El anterior marco legal fija los lineamientos para el tratamiento de datos de carácter personal y tiene por objeto establecer las medidas de índole técnica y organizativa necesarias para garantizar la seguridad que deben reunir las bases de datos, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal.

Oesía. Como Responsable del Tratamiento, ha implantado los procedimientos que se describen en el presente documento para garantizar la seguridad de los datos de carácter personal generados en el desarrollo de su actividad profesional.

2 Definiciones y Glosario de Términos

2.1 Definiciones

- **Fuente de información:** Es la entidad u organización que recibe o conoce los datos personales de los titulares de la información, en virtud de una relación comercial o de cualquier índole, que contando con la autorización del titular, suministra esos datos a un operador de la información, que a la vez se los entrega a un usuario final.

  Si la fuente entrega la información directamente a los usuarios sin relación de un operador, este tendrá la doble condición de fuente y operador y se sujetará a los deberes y responsabilidades.

- **Operador de la información:** Es quien recibe de la fuente datos sobre varios titulares de la información, los administra y pone en conocimiento de los usuarios.

  Salvo que el operador sea la misma fuente de información, este no tiene relación comercial o de servicio con el titular y por ende no es responsable de la calidad de los datos que le son suministrados por la fuente.

- **Usuario:** Es la persona natural o jurídica que puede acceder a la información suministrada por la fuente o el operador, o directamente por el titular de la información, en el caso que el usuario a su vez entregue información directamente a un operador, tendrá la doble condición de usuario y fuente y asumirá los deberes y responsabilidades de ambas partes.

- **Dato personal:** Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables, los datos personales pueden ser públicos, semiprivado o privados.

- **Dato público:** Son públicos entre otros los datos contenidos en documentos púbicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de la persona. Además de los que no sean privados o semiprivados.

- **Dato semiprivado:** Es semiprivado el dato que no tiene naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar a ciertos sectores o a la sociedad en general, como los datos financieros, crediticios, y de actividad comercial.

- **Dato privado:** Es el dato que por su naturaleza intima o reservada solo es relevante para el titular.

- **Datos sensibles:** Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación

política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

- **Agencia de Información comercial:** Es toda empresa constituida legalmente que tenga como actividad principal, la recolección, validación y procesamiento de información comercial, sobre empresas y comerciantes, solicitadas por sus clientes, entendiéndose por información comercial, la información histórica y actual relativa a la situación financiera, patrimonial, de mercado, administrativa, operativa, sobre el cumplimiento de las obligaciones y demás información relevante.

- **Autorización:** Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos.

- **Base de datos:** Conjunto organizado de datos personales que sea objeto de tratamiento.

- **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 de Tratamiento.

- **Titular:** Persona natural cuyos datos personales sean objeto de tratamiento.

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

- **Responsable:** Es la persona natural o jurídica que decide sobre la base de datos o el tratamiento de datos, ya sea por si sola o en sociedad con otros.

3 *Ámbito de Aplicación*

El presente documento será de aplicación a las bases que contienen datos de carácter personal que se hallan bajo la responsabilidad de **Oesía en Colombia,** a partir de ahora, **Oesía** incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en normativa vigente, las personas que intervienen en el tratamiento y las sedes en los que se ubican.

Cada uno de estos activos deberá estar sujeto a una serie de medidas de seguridad, las cuales varían en función del nivel de clasificación de seguridad de cada uno de ellos.

3.1 Bases con datos de carácter personal

A modo de relación se presenta las bases de datos sujetos a las medidas de seguridad establecidas en este documento, con indicación del nivel de seguridad correspondiente.

1	**CLIENTES**	**GESTIÓN COMERCIAL**	**B**
2	**OESÍA GO**	**CONTROL Y GESTIÓN DEL PERSONAL ASIGNACION A PROYECTOS E IMPUTACION DE HORAS**	**B**
3	**PERSONAL**	**CONTRATACION LABORAL, NOMINA Y SEGURIDAD SOCIAL GESTION DE PERSONAL CONTROL DE ACCESOS FISICOS Y LOGICOS GESTION DE GASTOS AUSENCIAS PRESENCIA LABORAL VACACIONES BENEFICIOS PARA EMPLEADOS FORMACION Y ACTUALIZACION DE DATOS CURRICULARES.**	**M**
4	**PREVENCION**	**COMUNICACIÓN, CONTROL E INVESTIGACION DE ACCIDENTES DE TRABAJO PARA EL SISTEMA DE GESTION INTEGRADO DE SEGURIDAD Y SALUD EN EL TRABAJO**	**A**
5	**SELECCIÓN DE PERSONAL**	**GESTION DE SELECCIÓN EN PROCESO DE SELECCION DE PERSONAL E INCORPORACIÓN DE PRACTICANTES Y PERSONAL SENA PARA LA PROPIA COMPAÑÍA O PARA CLIENTES DE OESÍA.**	**M**
6	**VISITAS**	**GESTION DE LAS VISITAS PLAZAS DE PARKING Y CONTROL DE ACCESO FISICO A LAS INSTALACIONES DE LA EMPRESA.**	**B**
7	**PROYECTOS**	**GESTION Y REALIZACIÓN DE PROYECTOS DE NEGOCIO PROPIOS Y DE TERCEROS**	**B**
8	**PROVEEDORES**	**CONTRATISTAS Y PROVEEDORES DE BIENES Y SERVICIOS**	**M**

3.2 Centros de tratamiento de la información

Se considera centro de tratamiento a aquella instalación donde se realizan operaciones y procedimientos técnicos, de carácter automatizado o no, que permiten la recogida, grabación, conservación, elaboración, modificación, bloqueo o cancelación de datos de carácter personal.

El conjunto de centros de tratamiento que comprende el alcance del presente Documento de protección de datos personales es el que se presenta a continuación.

GRUPO OESÍA BOGOTÁ (SEDE CENTRAL)	Cra 19 B No 82-46 pisos 2-3-4	Bogotá
GRUPO OESÍA FUNZA	Kilómetro 4 vía Siberia Parque industrial San José Bodega 15	Funza

3.3 Personal que interviene en el Tratamiento

El personal que interviene en el tratamiento de los datos de carácter personal, y que por tanto está autorizado a acceder a los sistemas de información, comprende en términos generales los siguientes perfiles:

- Personal de las Direcciones Organizativas. Este es el personal asignado a las distintas Direcciones, que gestionan los datos protegidos como parte de su trabajo.

- Personal de Administración de Sistemas. Este es el personal asignado que administra los sistemas y redes informáticas y conserva las bases de datos de la organización.

- Personal encargado del Archivo de Documentación en Papel. Este es el personal designado para encargarse de los archivos guardados en lugares comunes a toda **Oesía.**

- Cualquier otra persona que por razones de trabajo deba acceder a datos de carácter personal, y que, siendo previamente autorizada en función del trabajo, no esté incluida en estos supuestos, por el tiempo necesario para la realización de dichos trabajos.

4 Derechos de los titulares de Datos Personales

El Titular de los datos personales tendrá los siguientes derechos:

- Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. 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;

- Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento.

- Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales;

- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley 1581 de 2012 y las demás normas que la modifiquen, adicionen o complementen;

- 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. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a la ley 1581 de 2012 y a la Constitución;

- Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

5 Medidas de Seguridad

5.1 Medidas, Normas, Procedimientos, Reglas y Estándares Encaminado a Garantizar los Niveles de Seguridad sobre los datos personales

5.2 Exigidos en este Documento

Las medidas de seguridad referidas a continuación incluyen todos los niveles Básico, Medio y Alto.

Las medidas de seguridad definidas van encaminadas a proteger todas las bases, aplicaciones y herramientas y consulta, recursos del sistema operativo, redes de telecomunicaciones, soportes y equipos informáticos, gestionados, siempre y cuando, dichos recursos incidan sobre datos de carácter personal.

Todas las personas que tengan acceso a los datos de los bases, bien a través del sistema informático habilitado para acceder a los mismos, o bien a través de cualquier otro medio automatizado o no de acceso a los bases, se encuentran obligadas a cumplir lo establecido en el presente documento, y sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento.

Una copia o resumen de este documento estará disponible, para su conocimiento, por parte de cada persona en el E-GROUP de **Oesía**.

5.3 Identificación y Autenticación

El mecanismo de identificación y autenticación que será utilizado en los sistemas de información es el de introducción de código de usuario y contraseña. Cuando el estado de la tecnología no permita adoptar este medio de autenticación se adoptarán medidas equivalentes que garanticen la identificación y autenticación de los usuarios de forma inequívoca y personalizada.

No se utilizarán identificadores de usuario genéricos, cada usuario dispondrá de un identificador personal e intransferible que le identifique de forma inequívoca y que quedará autenticado mediante contraseñas que serán almacenadas siempre en formato ininteligible.

En el inicio de sesión para el acceso a los datos de los servidores para cada puesto (PC, portátil, etc) se obligará a introducir el usuario y contraseña personal.

Cada usuario será responsable de la confidencialidad de su contraseña, y en caso de que la misma sea conocida por personas no autorizadas de manera fortuita o fraudulenta, el usuario deberá comunicar este hecho para su registro como incidencia y se procederá inmediatamente a su cambio.

Siempre que los medios técnicos lo permitan, se forzará el cambio periódico de contraseñas al menos una vez al año. Cuando no sea posible automatizar este

requerimiento de caducidad, el usuario será responsable del cambio sistemático de las mismas, al menos una vez al año.

El personal externo que accede a los recursos de OESÍA, estará sometido a las mismas condiciones y obligaciones de seguridad que el personal interno.

5.3.1 Bases de Nivel Medio Y Alto

El sistema de autenticación de los sistemas de información limitará la posibilidad de intentar reiteradamente el acceso no autorizado. El número de intentos será el establecido por el área de TI.

5.3.2 Control de Accesos

Los usuarios recibirán sus derechos de acceso limitados, únicamente accederán a aquellos datos y recursos informáticos que precisen para el desarrollo de sus funciones. Al dar de alta un usuario, se le asociará un grupo correspondiente a su función que tendrá asociado unos permisos de accesos a carpetas de red que permitirán al usuario desarrollar su trabajo. Los accesos adicionales a los inherentes a un grupo deberán ser solicitados, y podrán ser autorizados o denegados previa revisión de los niveles de autorizaciones.

Los responsables de los sistemas y aplicaciones dotarán los medios para obtener una relación de usuarios actualizada que incluya el tipo de acceso autorizado para cada uno de ellos.

El personal externo que accede a los recursos de la organización estará sometido a las mismas condiciones y obligaciones de seguridad que el personal interno.

La información compartida de bases de datos ofimáticos se realizará a través de unidades de red y un sistema de carpetas que permita el control del acceso sólo a las personas autorizadas al tratamiento de la información que contenga.

Prestaciones de servicios sin acceso a datos personales.

Se adoptarán las medidas adecuadas para que el personal que realicen labores o trabajos que no impliquen el tratamiento a datos de carácter personal, no tengan acceso a los mismos ni a los soportes que los contengan o a los recursos de los sistemas de información que los trate.

Autorizaciones

Exclusivamente el personal autorizado que figura a continuación podrá conceder, alterar o anular el acceso autorizado sobre los recursos:

- **Responsable del área de TI Seguridad**
- **Cada área responsable de la base de datos**

5.3.3 Bases de Nivel Medio y Bajo

Acceso Físico

El acceso a la documentación y el acceso físico a las ubicaciones donde se encuentran los sistemas de archivo de documentos se limitarán exclusivamente al personal autorizado.

Se establecerán mecanismos para que sólo el personal autorizado pueda acceder a los lugares donde se encuentran instalados los equipos físicos que dan soporte a los sistemas de información con carácter general:

- Se archivarán los documentos en archivadores que dispongan de una puerta u otro mecanismo de cierre similar.
- Las llaves estarán en posesión de personas autorizadas que serán responsables de los documentos y velarán por que el acceso de otras personas esté autorizado.
- Los archivadores estarán ubicados en las zonas menos accesibles, alejados de espacios de tránsito y paso de otras personas, y bajo la directa supervisión visual de los responsables. Si los datos fuesen de nivel alto, se ubicarán en espacios independientes que tendrán a su vez puerta con cerradura que permanezcan cerrados al finalizar la jornada laboral.

5.3.4 Bases de Nivel Alto

Acceso a la documentación

El acceso a la documentación se limitará exclusivamente al personal autorizado. Los responsables de los archivos establecerán mecanismos para identificar los accesos cuando a estos documentos accedan múltiples usuarios.

Se registrarán los accesos de personal no autorizadas a la documentación, si se diese esta circunstancia.

Registro de accesos

Cuando se acceda a datos de nivel alto todos los sistemas gestores de información y de datos nivel alto de carácter personal registraran la siguiente información.

- Identificación del usuario.
- Fecha y hora en que se realizó el Acceso y la base accedida.
- Tipo de acceso.
- Constancia de si el acceso ha sido autorizado o denegado.
- En el caso de que el acceso haya sido autorizado, se registrará el identificador del registro accedido.

Esta información será conservada por un período de dos años y el Responsable del tratamiento se encargará anualmente de revisar la información de control registrada.

Los mecanismos que habilitan el mencionado registro de los accesos no podrán, bajo ningún concepto, ser desactivados.

5.4 Gestión de Soportes

Tendrá consideración de soporte cualquier objeto físico que almacena o contiene datos o documentos, u objetos susceptibles de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

Los soportes que contengan datos de carácter personal permitirán identificar el tipo de información que contienen, serán inventariados y almacenados en dependencias a la que solo tendrán acceso las personas debidamente autorizadas.

Todos los soportes de bases automatizados con independencia del nivel de seguridad que se le haya adjudicado serán identificados y enviados al área de TI, para la respectiva conservación, almacenamiento y back up de las mismas.

Solo con la autorización del Encargado de Tratamiento de datos personales podrán salir soportes y documentos que contengan datos de carácter personal, fuera de los locales de oesia

Dispositivos Portátiles

Los soportes que hoy en día se utilizan, (CD,USB, discos duros externos, portátiles, móviles etc), son capaces de albergar gran cantidad de información y son fácilmente transportables, es evidente la importancia de la seguridad de los datos contenidos en estos medios.

Como norma general, se limitará a los empleados el uso de soportes extraíbles en las oficinas de la organización. Cuando sea necesario utilizar soportes extraíbles para el

tratamiento de las bases, deberán ser adecuadamente etiquetados e identificados y responsablemente custodiados.

5.5 **Redes** de Comunicaciones

En los accesos en remoto a través de redes de comunicaciones públicas o privadas (LAN o WAN) se proveerán las medidas para que los usuarios que se conecte a los sistemas y aplicaciones a través de redes de comunicaciones (locales, corporativas o Internet) lo hagan de tal manera que solo puedan acceder a los mismos datos a los que tenga acceso en modo local y para aquellos ámbitos para los que esté autorizado.

Cuando existan procedimientos de acceso remoto se realizarán bajo identificación y autenticación de los usuarios, sin que se permita la existencia de usuarios genéricos que dispongan de acceso a los sistemas sin ser identificados, y en general se realizará de tal manera que garantice un nivel de seguridad equivalente al que corresponde a los bases en los accesos en modo local.

Accesos vía VPN

El acceso a los datos desde el exterior se llevará a cabo a través de una conexión VPN protegida o similar mitigando el riesgo de filtración de la información. Este acceso está restringido por medio de la instalación de software y de un certificado concreto.

5.6 Régimen de trabajo fuera de los locales de la ubicación de las bases que contienen datos personales fichero

Cuando se realicen trabajos externos a las instalaciones fuera de los locales de ubicación física de los bases, se guardarán las normas de seguridad sobre accesos remotos que se han especificado en el apartado **Redes de Comunicaciones**.

Ordenadores portátiles

Cuando los trabajos se realicen con ordenadores portátiles propiedad de **Oesía** o de sus colaboradores, será obligatorio que se hayan habilitado sistemas de identificación y autenticación por contraseña.

La persona responsable de la utilización del equipo seguirá las normas establecidas al efecto por **Oesía** en cuanto medidas de seguridad se refiere y se encargará de definir y modificarla contraseña y cambiarla con la periodicidad establecida en el Documento de tratamiento y protección de datos personales

A esto se añadirán las medidas de seguridad especificadas en el apartado de Gestión de Soportes para dispositivos portátiles.

Autorizaciones

Se autoriza al personal que dispone de dispositivos portátiles para llevar a cabo el tratamiento de datos de carácter personal fuera de las propias instalaciones de Oesía acorde a la finalidad concreta y determinada del trabajo encomendado. Esta autorización tiene carácter indefinido y regirá durante el tiempo necesario para la ejecución del servicio.

De la misma manera se autorizan los accesos vía VPN a los empleados que hayan de realizar tareas en remoto por el tiempo necesario para los trabajos a realizar. Si la naturaleza de las tareas necesitase una conexión permanente se considerará que esta autorización tiene un carácter indefinido con la finalización de la relación del empleado con la empresa.

Traslado de Documentación

Siempre que se proceda al traslado físico de la documentación contenida en un archivo físico o digital, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

5.7 Información y Concienciación

Oesía velará por la concienciación e información de los empleados en la descarga y tratamiento de datos de carácter personal en ubicaciones no seguras como discos duros, lugares en la nube no controlados, dispositivos removibles etc.

5.7.1 Bases de Nivel Alto

La realización de copias o reproducción de los documentos con datos de carácter personal solo podrá ser realizada bajo el control del personal autorizado.

Autorizaciones

Se autoriza al personal del departamento de Recursos Humanos, Administración de Personal y Compras para la copia o reproducción de documentos con datos de carácter personal dentro del ámbito de su competencia y de forma proporcionada a las necesidades de las tareas que desempeñan.

5.8 Procedimientos copias de respaldo y recuperación

Para garantizar la integridad y la disponibilidad de los datos de carácter personal se establecerán procesos de copias de respaldo y de recuperación que en caso de fallo o incidencia que produzca una pérdida de datos accidental, permitan recuperar y en su caso reconstruir los datos de los bases. Estos procesos cumplirán al menos los siguientes apartados:

- Se deberá obtener semestralmente una copia de seguridad de los bases, a efectos de respaldo y posible recuperación en caso de fallo.

- En caso de pérdida total o parcial de los datos de los bases existirá un procedimiento, informático parametrizado (un manual), que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, es capaz de reconstruir los datos de los bases y dejarlos en el estado en que se encontraban en el momento del fallo.

5.8.1 Bases de Nivel Alto

Se conservará una copia de respaldo de los datos y una copia de los procedimientos de recuperación en un lugar diferente de aquél en que se ubiquen habitualmente los mismos, pero que conserve las medidas de seguridad necesarias, o si por la naturaleza de las instalaciones no fuese posible, se habilitarán medios alternativos que permita asegurar la conservación de dicha copia y procedimiento.

Procedimiento de Restauración de datos

El Responsable de los datos o en su caso la persona por él designada, se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

En su defecto se aportará evidencias de que se han realizado restauraciones reales en un plazo inferior a los seis meses reglamentariamente establecidos.

Custodia de los documentos.

En tanto los documentos con datos personales que no se encuentren archivados en sus dispositivos de almacenamientos, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo las personas que se encuentren a su cargo deberán custodiarlo e impedir en todo momento que pueda ser accedido por personas no autorizadas.

En el traslado de la documentación entre departamentos, esta será portada en una carpeta de tal manera que no se pueda ver desde el exterior la información de los documentos y que no sea posible su perdida accidental o sustracción malintencionada.

Acceso a la documentación

El acceso a la documentación se limitará exclusivamente al personal autorizado. Los responsables de los archivos establecerán mecanismos para identificar los accesos cuando a estos documentos accedan múltiples usuarios y se establecerá un registro para dejar constancia de accesos por parte de personas no autorizadas que pudieran ocurrir.

Traslado de Documentación

Siempre que se proceda al traslado físico de soportes o documentos, se adoptarán las medidas dirigidas a evitar la sustracción, pérdida, acceso indebido a la información durante su transporte.

Cuando se trate de traslado de documentos dentro de las propias instalaciones, se realizará de tal manera que la documentación no esté a la vista de personas ajenas al proceso, transportándolos en una carpeta y que no permita la perdida accidental de los documentos en cuestión. Dicho contenedor (carpeta cerrada, caja, portafolios, etc.) debe estar siempre bajo la custodia de la persona que realiza el trámite.

Autorizaciones

Los responsables que tienen autorización para acceder a documentos de nivel alto y realizar copias o reproducciones de los mismos son los siguientes:

- **El Responsable de cada área.**
- **Las personas delegadas por el mismo.**

5.9 Prestación de servicios sin tratamiento de datos de carácter personal

Como parte de sus funciones, **Oesía** puede contratar la prestación de servicios por parte de terceros, sin que esta prestación conlleve el tratamiento de datos de carácter personal.

Se prohíbe terminantemente todo acceso y tratamiento de cualquier tipo de información confidencial y, en concreto, de los datos de carácter personal responsabilidad de **Oesía** por parte del prestador.

No obstante, en el supuesto de que el personal externo llegará a conocer accidentalmente cualquier tipo de información confidencial con objeto de la prestación del servicio, estará obligado a guardar secreto respecto de la misma, no divulgarla ni publicarla, bien directamente, bien a través de terceras personas o empresas, o a ponerla a disposición de terceros. Este compromiso de confidencialidad tiene carácter indefinido, subsistiendo tras la finalización de la prestación de servicio.

El prestador comunicará y hará cumplir al personal a su cargo y contratado por su cuenta, las obligaciones establecidas en el presente Documento.

6 *Publicidad de la Política de Tratamiento de Datos Personales*

La presente política estará publicada en la página de internet de la sociedad http://grupooesia.com/grupo-oesia-colombia-2/, cada cambio que se haga a la misma será enviado en la nueva versión a los correos corporativos de los Empleados y contratistas indicando los cambios que sufrió la política.

7 *Información y Obligaciones del Personal*

Todo el personal que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.

7.1 Información al personal

Se adoptarán las medidas necesarias para que el personal actual o el que en el futuro se incorpore conozca las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Se informará al personal de sus obligaciones de acuerdo con la normativa sobre protección de datos por los siguientes medios:

- El personal podrá acceder a la documentación relacionada con la normativa de protección de datos a través del E-GROUP o la página http://grupooesia.com/grupo-oesia-colombia-2/.
- Todo el personal con el contrato firmará una cláusula de autorización de datos personales ya sea en el contrato laboral o como anexo. Previo a la vinculación
- Los empleados ya vinculados firmarán ANEXO de autorización de datos personales donde otorgan su consentimiento retroactivo desde la fecha de ingreso de las personas.

Responsable de Seguridad

Oesía será el Responsable del tratamiento de datos personales quien tendrá los siguientes deberes

1. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;

2. Solicitar y conservar, en las condiciones previstas en la ley 1581 del 2012 y las normas que la desarrollan, copia de la respectiva autorización otorgada por el Titular

3. Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada

4. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento

5. Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;

6. 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;

7. Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.

8. Suministrar al Encargado del Tratamiento según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley;

9. Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;

10. Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley;

11. 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;

12. 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;

13. Informar a solicitud del Titular sobre el uso dado a sus datos;

14. 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.
15. Cumplir las instrucciones y requerimientos que impartan las Superintendencias de Industria y Comercio.

Encargados del tratamiento

Oesía nombrara como encargado de tratar datos de carácter personal a las áreas gestoras de cada base de datos, quienes tendrán como deberes los siguientes, sin perjuicio de las demás disposiciones previstas en la ley y en otras que rijan su actividad:

1. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de HÁBEAS DATA.

2. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

3. Actualizar la información reportada por los responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;

4. Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la ley;

5. 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 por parte de los Titulares;

6. Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la ley;

7. Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal

8. Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio;

9. Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella;

10. Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;

PARÁGRAFO 1. En el evento en que concurran las calidades de Responsable del Tratamiento y Encargado del Tratamiento en la misma persona, le será exigible el cumplimiento de los deberes previstos para cada uno.

PARÁGRAFO 2. Oesía velará para que los Encargados del Tratamiento de Datos Personales den cumplimiento a las obligaciones aquí establecidas.

Funciones para los empleados

El personal afectado por esta normativa se clasifica en los siguientes perfiles:

Administradores. Red, Sistemas Operativos y Bases de Datos

Serán los responsables de los máximos privilegios y por tanto del máximo riesgo de que una actuación errónea pueda afectar al sistema. Tendrán acceso al software (programas y datos) del sistema, a las herramientas necesarias para su trabajo y a los bases necesarios para resolver los problemas que surjan.

Son los encargados de administrar o mantener el entorno operativo de los Bases automáticos. Por sus funciones pueden utilizar herramientas de administración que permitan el acceso a los datos protegidos eludiendo los controles o barreras de acceso de la Aplicación.

Se encargarán además del mantenimiento de los sistemas y aplicaciones y de la resolución de incidencias que puedan surgir en el entono hardware / software de los sistemas informáticos o de la propia aplicación de acceso al Fichero.

Usuarios.
Personal que usualmente utiliza el sistema informático de acceso a los datos para el desempeño de su trabajo. Son empleados de la empresa cuyo cometido es el tratamiento de los datos en labores administrativas, comerciales, de gestión interna o en áreas especializadas que acceden a los datos y los mantienen en función de su puesto de trabajo.

7.1.1 Obligaciones

Las obligaciones que se recogen a continuación tienen carácter general y no depende de la pertenencia a los perfiles que se han establecido en el anterior apartado.

Todas las personas que intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligadas al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular de los datos o, en su caso, con el responsable del mismo.

Como norma general las personas que intervengan en cualquier fase del tratamiento de bases que contengan datos de carácter personal, deben cumplir las normas, directivas y procedimientos que establezca **Oesía** en materia de protección de datos personales, además de velar en todo momento por la calidad e integridad de los datos personales y desarrollar su actividad en el entorno más seguro de cuantos sea posible.

Constituye una obligación del personal notificar al Responsable de los datos personales de las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este documento.

Prestarán especial atención a la observación de las obligaciones relacionadas con:

- Confidencialidad de la información.
- Mantenimiento de la seguridad del puesto de trabajo.
- Protección de las contraseñas personales.

Prestaciones de servicios sin acceso a datos personales.

Se limitará a lo indispensable el acceso de personal ajeno a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos de limpieza, mantenimiento, vigilancia o similares.
Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

7.1.2 Consecuencias del incumplimiento del documento de seguridad

El personal Interno que incumplan cualquiera de las funciones y obligaciones descritas en este documento se le aplicará las medidas disciplinarias que en su caso procedan, siendo sancionados conforme a la normativa interna o externa que en cada caso aplique a incumplimiento cometido.

8 Procedimiento de Gestión y Respuestas ante las Incidencias

8.1 De conformidad con lo dispuesto en el Artículo 20 del decreto 1377 de 2013, los derechos de los Titulares establecidos en la Ley, podrán ejercerse por:

- El Titular, deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el Responsable.
- Por sus causahabientes, quienes deberán acreditar la calidad.
- Por el representante y/o apoderado del Titular, previa acreditación de la representación y apoderado.

Los Titulares o causahabientes podrán consultar la información personal del Titular que repose en cualquier base de datos de OESÍA, quien suministrara a estos toda la información contenida en el registro individual o que esté vinculada con la identificación del Titular.

8.2 Consultas: Los Titulares o sus causahabientes pueden consultar la información personal del Titular que repose en cualquiera base de datos de OESÍA, quien suministrara a estos toda la información contenida en el registro individual o que esté vinculada con la identificación del Titular.

8.3 Término: La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, su consulta expresada los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días siguientes al vencimiento del primer término.

8.4 Reclamos: El Titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de: corrección, o supresión, podrán presentar un reclamo ante OESÍA bajo la siguiente información:

a. La identificación del Titular.

b. La descripción de los hechos que dan lugar al reclamo.

c. La dirección, y acompañando los documentos que se requiera hacer valer.

d. Si el reclamo resulta incompleto se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo 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 quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponde en termino máximo de 2 (dos) días hábiles informará de la situación al interesado.

Una vez recibido el reclamo completo, el mismo se gestionará en un término no mayor a 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, lo cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término. Si vencido el término legal respectivo, OESÍA no hubiese eliminado corregido los datos personales, el Titular tendrá derecho a solicitar a la Superintendencia de Industria y Comercio que ordene la revocatoria de la autorización y/o a la supresión de los datos personales, de acuerdo con el procedimiento descrito en el artículo 22 de la ley 1581 del 2012.

La petición o derecho que ejercita el Titular de los datos personales, debe contener nombres y apellidos del usuario y los datos del contacto para recibir notificaciones. Este derecho se podrá ejercer entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté prohibido o no haya sido autorizado por su Titular.

9 *Vigencia*

La vigencia de la Política de Tratamiento y Protección de Datos Personales, estará vigente a partir de su publicación y durante el tiempo que OESÍA ejerza las actividades propias de su objeto social.

Para cualquier información relativa a esta Política de Protección de datos puede acercarse a la dirección Carrera 19 B No. 82-46, o enviar una comunicación al correo electrónico: protecciondatos@oesia.com