



# MANUAL DE POLÍTICAS Y PROCEDIMIENTOS

*Ley 1581 de 2012 de Protección de Datos Personales*

*Última actualización: febrero de 2024*



## ÍNDICE

1. BASE LEGAL Y ÁMBITO DE APLICACIÓN
2. DEFINICIONES.
3. AUTORIZACIÓN DE LA POLÍTICA DE TRATAMIENTO.
4. RESPONSABLE DEL TRATAMIENTO
5. TRATAMIENTO Y FINALIDADES DE LAS BASES DE DATOS
6. DERECHOS DE LOS TITULARES
7. ATENCIÓN A LOS TITULARES DE LAS BASES DE DATOS
8. PROCEDIMIENTOS PARA EJERCER LOS DERECHOS DEL TITULAR
  - 8.1 DERECHO DE ACCESO O CONSULTA
  - 8.2 DERECHOS DE QUEJAS Y RECLAMO
9. MEDIDAS DE SEGURIDAD
10. OBLIGACIONES DEL RESPONSABLE
11. CONOCIMIENTO DE LA POLÍTICA
12. MECANISMOS DE RECOLECCIÓN DE DATOS
13. TRANSFERENCIA DE DATOS A TERCEROS PAÍSES
14. VIGENCIA DE LA POLÍTICA Y LAS BASES DE DATOS



## 1. BASE LEGAL Y ÁMBITO DE APLICACIÓN

La política de tratamiento de la información se desarrolla en cumplimiento de los **artículos 15 y 20 de la Constitución Política; de los artículos 17, literal k), y 18, literal f), de la Ley Estatutaria 1581 de 2012**, “Por la cual se dictan disposiciones generales para la Protección de Datos Personales” (en adelante LEPD); y del **artículo 13 del Decreto Único reglamentario 1074 de 2015, Decreto 090 de 2018, Circular 003 de 2018**, emitida por la Superintendencia de Industria y Comercio y demás normas concordantes

Esta política será aplicable a todos los datos personales registrados en bases de datos que sean objeto de tratamiento por el responsable del tratamiento.

Esta política será aplicable a todos los datos personales registrados en bases de datos que sean objeto de tratamiento por el responsable del tratamiento.

Los datos de las personas relacionadas con **(LA/FT/FPDAM) Lavado de Activos, Financiación del Terrorismo y Proliferación de Armas de Destrucción Masiva**, se tratarán conforme a la Ley y cuando corresponda serán reportados ante la **UIAF** y transferidos a entidades de control y vigilancia que los soliciten.

## 2. DEFINICIONES ESTABLECIDAS EN EL ARTÍCULO 3 DE LA LEPD Y EL ARTÍCULO - 2.2.2.25.1.3. DEL DECRETO 1074 DE 2015

- i. **AUTORIZACIÓN:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.
- ii. **BASE DE DATOS:** Conjunto organizado de datos personales que sea objeto de tratamiento.
- iii. **DATO PERSONAL:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- iv. **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.

- v. **DATOS SENSIBLES:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.
- vi. **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.
- vii. **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.
- viii. **TITULAR:** Persona natural cuyos datos personales sean objeto de tratamiento.
- ix. **TRATAMIENTO:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- x. **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.



- xI. **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.
- xII. **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.

### 3. AUTORIZACIÓN DE LA POLÍTICA DE TRATAMIENTO

De acuerdo con el artículo 9 de la LEPD, para el tratamiento de datos personales se requiere la autorización previa e informada del Titular. Mediante la aceptación de la presente política, todo Titular que facilite información relativa a sus datos personales está consintiendo el tratamiento de sus datos por parte del **FONDO DE EMPLEADOS DE ORACLE**, en los términos y condiciones recogidos en la misma.

No será necesaria la autorización del Titular cuando se trate de:

- I. Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- II. Datos de naturaleza pública.
- III. Casos de urgencia médica o sanitaria.
- IV. Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- V. Datos relacionados con el Registro Civil de las personas.
- VI. A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.
- VII. Las que tengan por finalidad la seguridad y defensa nacional la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo.



- viii. Las que tengan como fin y contengan información de inteligencia y contrainteligencia.
- ix. Las que contengan información periodística y otros contenidos editoriales
- x. Las bases de datos con información financiera, crediticia, comercial y de servicios, y de los censos de población y vivienda.

#### 4. RESPONSABLE DEL TRATAMIENTO

El responsable del tratamiento de las bases de datos objeto de esta política es el **FONDO DE EMPLEADOS DE ORACLE**, cuyos datos de contacto son los siguientes:

- Dirección: Calle 127 a 53ª - 45 Torre 2 de la ciudad de Bogotá D.C.
- Correo electrónico: [servicios@feoracle.com.co](mailto:servicios@feoracle.com.co)
- Teléfono: 6451051 -3587173 – 32091956680
- Pagina web: <https://www.feoracle.com.co/>

#### 5. TRATAMIENTO Y FINALIDADES DE LAS BASES DE DATOS

El **FONDO DE EMPLEADOS DE ORACLE**, en el desarrollo de su actividad empresarial, lleva a cabo el tratamiento de datos personales relativos a personas naturales que están contenidos y son tratados en bases de datos destinadas a finalidades legítimas, cumpliendo con la Constitución y la Ley.

La siguiente tabla (Tabla I) presenta las distintas bases de datos que manejan la empresa y las finalidades asignadas a cada una de ellas.

**TABLA I. BASES DE DATOS Y FINALIDADES**

| <b>BASE DE DATOS</b> | <b>FINALIDAD</b>  | <b>FINALIDAD – Superintendencia de Industria y Comercio</b>   |
|----------------------|---|---|
| <b>ASOCIADOS</b>     | Recolección, custodia, almacenamiento, tratamiento y de datos personales de empleados y Asociados con el fin de gestionar reportes de pagos, seguimiento, aportes, novedades de nómina, control de horarios, aportes legales, capacitaciones, formación del personal, gestión de prevención de riesgos laborales, consulta en listas de antecedentes penales y judiciales | <ul style="list-style-type: none"> <li>• Gestión contable, fiscal y administrativa - Gestión administrativa</li> <li>• Actividades asociativas, culturales, recreativas, deportivas y sociales - Gestión de asociados o miembros de partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro</li> <li>• Finalidades varias – Custodia y gestión de información y bases de datos</li> </ul> |
| <b>BENEFICIARIOS</b> | Recolección, custodia, almacenamiento, tratamiento y de datos personales de beneficiarios con el fin de realizar y gestionar actividades asociativas, culturales y demás.   | <ul style="list-style-type: none"> <li>• Finalidades varias - Gestión de estadísticas internas</li> <li>• Información de Empleados</li> <li>• Actividades asociativas, culturales, recreativas, deportivas y sociales - Asistencia social</li> </ul>  |
| <b>PROVEEDORES</b>   | Recolección, custodia, almacenamiento, tratamiento y de datos personales con el fin de gestionar convenios, establecer relaciones comerciales con terceros que proveen y suministran al fondo cualquier clase de Servicio y/o bien.   | <ul style="list-style-type: none"> <li>• Descripción de la Finalidad Gestión contable, fiscal y administrativa - Gestión de proveedores y contratistas</li> <li>• Gestión contable, fiscal y administrativa - Gestión administrativa</li> </ul>   |
| <b>DECSIS</b>        | Recolección, custodia, almacenamiento, tratamiento y de datos personales con el fin de gestionar todo lo relativo a información de créditos ahorros y aportes de los asociados.   | <ul style="list-style-type: none"> <li>• Gestión contable, fiscal y administrativa - Gestión económica y contable</li> <li>• Gestión contable, fiscal y administrativa - Gestión administrativa</li> </ul>  |

## 6. DERECHOS DE LOS TITULARES

De acuerdo con lo previsto en el artículo 8 de la LEPD y los artículos 2.2.2.25.4.3. y 2.2.2.25.4.4. del Decreto 1074 de 2015, los Titulares de los datos pueden



ejercer una serie de derechos en relación con el tratamiento de sus datos personales.

Estos derechos podrán ejercerse por las siguientes personas.

- i. Por el Titular, quién deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.
- ii. Por sus causahabientes, quienes deberán acreditar tal calidad.
- iii. Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.
- iv. Por estipulación a favor de otro y para otro.

Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

Los derechos del Titular son los siguientes:

- **DERECHO DE ACCESO O CONSULTA:** Se trata del derecho del Titular a ser informado por el responsable del tratamiento, previa solicitud, respecto al origen, uso y finalidad que le han dado a sus DATOS personales.
- **DERECHOS DE QUEJAS Y RECLAMOS.** La Ley distingue cuatro tipos de reclamos:
  - **RECLAMO DE CORRECCIÓN:** el derecho del Titular a que se actualicen, rectifique o modifiquen aquellos datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
  - **RECLAMO DE SUPRESIÓN:** el derecho del Titular a que se supriman los datos que resulten inadecuados, excesivos o que no respeten los principios, derechos y garantías constitucionales y legales.
  - **RECLAMO DE REVOCACIÓN:** el derecho del Titular a dejar sin efecto la autorización previamente prestada para el tratamiento de sus datos personales.
  - **RECLAMO DE INFRACCIÓN:** el derecho del Titular a solicitar que se subsane el incumplimiento de la normativa en materia de Protección de Datos.





- **DERECHO A SOLICITAR PRUEBA DE LA AUTORIZACIÓN OTORGADA AL RESPONSABLE DEL TRATAMIENTO:** salvo cuando expresamente se exceptúe como requisito para el tratamiento de conformidad con lo previsto en el artículo 10 de la LEPD.
- **DERECHO A PRESENTAR ANTE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO QUEJAS POR INFRACCIONES:** el Titular o causahabiente solo podrá elevar esta queja una vez haya agotado el trámite de consulta o reclamo ante el responsable del tratamiento o encargado del tratamiento.

## 7. ATENCIÓN A LOS TITULARES DE DATOS

El **FONDO DE EMPLEADOS DE ORACLE**, ha delegado a un responsable quien será en adelante el encargado de responder a peticiones, consultas y reclamos ante la cual el Titular de los datos puede ejercer sus derechos.

Teléfono: 6451051 -3587173 - 3209195668, correo electrónico: [servicios@feoracle.com.co](mailto:servicios@feoracle.com.co)

## 8. PROCEDIMIENTOS PARA EJERCER LOS DERECHOS DEL TITULAR

### 8.1. Derecho de acceso o consulta

Según el artículo 2.2.2.25.4.2. del Decreto Único reglamentario 1074 de 2015, el Titular podrá consultar de forma gratuita sus datos personales en dos casos:

- Al menos una vez cada mes calendario.
- Cada vez que existan modificaciones sustanciales de las políticas de tratamiento de la información que motiven nuevas consultas.

Para consultas cuya periodicidad sea mayor a una por cada mes calendario, el **FONDO DE EMPLEADOS DE ORACLE**, solamente podrá cobrar al Titular gastos de envío, reproducción y, en su caso, certificación de documentos. Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente. Para tal efecto, el responsable deberá demostrar a la Superintendencia de Industria y Comercio, cuando ésta así lo requiera, el soporte de dichos gastos.



El Titular de los datos puede ejercitar el derecho de acceso o consulta de sus datos mediante un escrito dirigido al **FONDO DE EMPLEADOS DE ORACLE**, enviado al correo electrónico a [servicios@feoracle.com.co](mailto:servicios@feoracle.com.co), indicando en el Asunto “Ejercicio del derecho de acceso o consulta”, o a través de correo postal remitido a la dirección Calle 127 a 53ª - 45 Torre 2 de la ciudad de Bogotá D.C. La solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- fotocopia de la cédula de ciudadanía del titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Petición en que se concreta la solicitud de acceso o consulta.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada, cuando corresponda.

El Titular podrá elegir una de las siguientes formas de consulta de la base de datos para recibir la información solicitada:

- Visualización en pantalla.
- Por escrito, con copia o fotocopia remitida por correo certificado o no.
- Tele copia.
- Correo electrónico u otro medio electrónico.
- Otro sistema adecuado a la configuración de la base de datos o a la naturaleza del tratamiento, ofrecido por el **FONDO DE EMPLEADOS DE ORACLE**.

Una vez recibida la solicitud, al **FONDO DE EMPLEADOS DE ORACLE**, resolverá la petición de consulta en un plazo 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, expresando 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 hábiles



siguientes al vencimiento del primer término. Estos plazos están fijados en el artículo 14 de la LEPD.

Una vez agotado el trámite de consulta, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

### *8.2. Derechos de quejas y reclamos*

El Titular de los datos puede ejercitar los derechos de reclamo sobre sus datos mediante un escrito dirigido al **FONDO DE EMPLEADOS DE ORACLE**, enviado al correo electrónico [servicios@feoracle.com.co](mailto:servicios@feoracle.com.co), indicando en el Asunto, “Ejercicio del derecho de acceso o consulta”, o a través de correo postal remitido a la dirección Calle 127 a 53ª - 45 Torre 2 de la ciudad de Bogotá D.C.

La solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- Fotocopia de la cédula de ciudadanía del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Descripción de los hechos y petición en que se concreta la solicitud de corrección, supresión, revocación o infracción.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada que se quieran hacer valer, cuando corresponda.

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.

Una vez recibido el reclamo completo, se incluirá en la base de datos 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.

Al **FONDO DE EMPLEADOS DE ORACLE**, resolverá la petición de consulta en un plazo máximo de quince (15) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender al 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.

Una vez agotado el trámite de reclamo, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

## **9. MEDIDAS DE SEGURIDAD**

Al **FONDO DE EMPLEADOS DE ORACLE**, con el fin de cumplir con el principio de seguridad consagrado en el artículo 4 literal g) de la LEPD, ha implementado medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Por otra parte, del **FONDO DE EMPLEADOS DE ORACLE**, mediante la suscripción de los correspondientes contratos de transmisión, ha requerido a los encargados del tratamiento con los que trabaja la implementación de las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de la información en el tratamiento de los datos personales.

A continuación, se exponen las medidas de seguridad implantadas por el **FONDO DE EMPLEADOS DE ORACLE**, que están recogidas y desarrolladas en su Manual Interno de Seguridad (Tablas II, III, IV y V).

## **10. OBLIGACIONES DEL RESPONSABLE**

Tanto el responsable del tratamiento como encargados, empleados, contratistas y demás terceros que actúen en nombre y representación del **FONDO DE EMPLEADOS DE ORACLE**., y tratan datos personales por disposición de ésta,



deben observar y respetar estas políticas en el cumplimiento de sus funciones y/o actividades aún después de terminados los vínculos legales, comerciales, laborales o de cualquier índole.

- i. De igual manera, se comprometen a guardar estricta confidencialidad en relación con los datos tratados. Por ende, deben obrar de tal forma que cumplan las siguientes obligaciones:
- ii. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- iii. Solicitar y conservar, en las condiciones previstas en la ley, copia de la respectiva autorización otorgada por el Titular.
- iv. Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
- v. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- vi. Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- vii. 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.
- viii. Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.
- ix. Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la ley.
- x. Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
- xi. Tramitar las consultas y reclamos formulados en los términos señalados en la ley.



- xii. Adoptar políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y en especial, para la atención de consultas y reclamos.
- xiii. 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.
- xiv. Informar a solicitud del Titular sobre el uso dado a sus datos.
- xv. 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.
- xvi. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.
- xvii. Deber de confidencialidad, el **FONDO DE EMPLEADOS DE ORACLE**, tratará como información confidencial todos los datos personales recolectados de manera manual o digital en sus bases de datos para lo cual: Suscribirá con sus empleados acuerdos de confidencialidad, Implementará medidas de protección de confidencialidad de conformidad con su Política de Procedimientos, exigirá a aquellos receptores de los datos personales cuando exista transferencia y/o transmisión de información, que el responsable o encargado cumpla con las respectivas obligaciones de confidencialidad.

## 11. CONOCIMIENTO DE LA PRESENTE POLÍTICA

Lo titulares de los datos podrán tener acceso a la política de tratamiento de datos personales a través de la página web del **FONDO DE EMPLEADOS DE ORACLE**., o realizando la solicitud de esta, mediante correo electrónico.

página web: <https://www.feoracle.com.co>

Correo electrónico: [servicios@feoracle.com.co](mailto:servicios@feoracle.com.co).



## 12. MECANISMOS DE RECOLECCIÓN DE DATOS

**FONDO DE EMPLEADOS DE ORACLE.**, utiliza para la recolección de los datos personales objeto de tratamiento, formatos físicos contacto cero con el titular de los datos y de manera digital, por medio de la página web. para cada uno de los casos **FONDO DE EMPLEADOS DE ORACLE**, ha indicado cuales son los mecanismos de información sobre los canales de atención, las finalidades para las cuales se recogen los datos y los derechos que, como titular se pueden ejercer; así como también los medios por los cuales pueden consultar la Política de tratamiento implementada.



**Tabla II. Medidas de seguridad comunes para todo tipo de datos (públicos, semiprivados, privados, sensibles) y bases de datos (automatizadas, no automatizadas)**

| Gestión de documentos y soportes   | Control de acceso   | Incidencias   | Personal  | Manual Interno de Seguridad   |
|--|---|---|---|---|
| <p>1. Medidas que eviten el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruidos.</p> <p>2. Acceso restringido al lugar donde se almacenan los datos.</p> <p>3. Autorización del responsable para la salida de documentos o soportes por medio físico o electrónico.</p> <p>4. Sistema de etiquetado o identificación del tipo de información.</p> <p>5. Inventario de soportes.</p> | <p>1. Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones.</p> <p>2. Lista actualizada de usuarios y accesos autorizados.</p> <p>3. Mecanismos para evitar el acceso a datos con derechos distintos de los autorizados.</p> <p>4. Concesión, alteración o anulación de permisos por el personal autorizado</p> | <p>1. Registro de incidencias: tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras.</p> <p>2. Procedimiento de notificación y gestión de incidencias.</p> | <p>1. Definición de las funciones y obligaciones de los usuarios con acceso a los datos</p> <p>2. Definición de las funciones de control y autorizaciones delegadas por el responsable del tratamiento.</p> <p>3. Divulgación entre el personal de las normas y de las consecuencias del incumplimiento de las mismas</p> | <p>1. Elaboración e implementación del Manual de obligatorio cumplimiento para el personal.</p> <p>2. Contenido mínimo: ámbito de aplicación, medidas y procedimientos de seguridad, funciones y obligaciones del personal, descripción de las bases de datos, procedimiento ante incidencias, procedimiento de copias y recuperación de datos, medidas de seguridad para el transporte, destrucción y reutilización de documentos, identificación de los encargados del tratamiento.</p> |



**TABLA III. MEDIDAS DE SEGURIDAD COMUNES PARA TODO TIPO DE DATOS (PÚBLICOS, SEMIPRIVADOS, PRIVADOS, SENSIBLES) SEGÚN EL TIPO DE BASES DE DATOS**

| BASES DE DATOS NO AUTOMATIZADAS  |   |  | BASES DE DATOS AUTOMATIZADAS  |   |
|--|---|--|---|---|
| ARCHIVO  | ALMACENAMIENTO DE DOCUMENTOS  | CUSTODIA DE DOCUMENTOS   | IDENTIFICACIÓN Y AUTENTICACIÓN  | TELECOMUNICACIONES                        |
| 1. Archivo de documentación siguiendo procedimientos que garanticen una correcta conservación, localización y consulta y permitan el ejercicio de los derechos de los Titulares. | 1. Dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas. | 1. Deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de los mismos. | 1. Identificación personalizada de usuarios para acceder a los sistemas de información y verificación de su autorización.<br><br>2. Mecanismos de identificación y autenticación;<br>Contraseñas: asignación, caducidad y almacenamiento cifrado. | 1. Acceso a datos mediante redes seguras. |

**TABLA IV. MEDIDAS DE SEGURIDAD PARA DATOS PRIVADOS SEGÚN EL TIPO DE BASES DE DATOS**

| BASES DE DATOS AUTOMATIZADAS Y NO AUTOMATIZADAS   |   |   | BASES DE DATOS AUTOMATIZADAS  |  |  |  |
|---|---|---|---|--|--|--|
| AUDITORÍA   | RESPONSABLE DE SEGURIDAD  | MANUAL INTERNO DE SEGURIDAD             | GESTIÓN DE DOCUMENTOS Y SOPORTES  | CONTROL DE ACCESO  | IDENTIFICACIÓN Y AUTENTICACIÓN   | INCIDENCIAS  |
| 1. Auditoría ordinaria (interna o externa) cada dos meses.                                  | 1. Designación de uno o varios responsables de seguridad.   | 1. Controles periódicos de cumplimiento | 1. Registro de entrada y salida de documentos y soportes:   | 1. Control de acceso al lugar o lugares donde se ubican los sistemas de información. | 1. Mecanismo que limite el número de intentos reiterados de acceso no autorizados. | 1. Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente. |
| 2. Auditoría extraordinaria por modificaciones sustanciales en los sistemas de información. | 2. Designación de uno o varios encargados del control y la coordinación de las medidas del Manual Interno de Seguridad. |   | fecha, emisor y receptor, número, tipo de información, forma de envío, responsable de la recepción o entrega. |  |  | 2. Autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación.                                 |
| 3. Informe de detección de deficiencias y propuesta de correcciones.                        | 3. Prohibición de delegación de la responsabilidad del responsable del tratamiento en el responsable de seguridad.      |   |   |  |  |  |
| 4. Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento.  |   |   |   |  |  |  |
| 5. Conservación del Informe a disposición de la autoridad.                                  |   |   |   |  |  |  |

**TABLA V. MEDIDAS DE SEGURIDAD PARA DATOS SENSIBLES SEGÚN EL TIPO DE BASES DE DATOS**

| BASES DE DATOS NO AUTOMATIZADAS   |  |   |  | BASES DE DATOS AUTOMATIZADAS   |  |   |
|---|--|---|--|--|--|---|
| CONTROL DE ACCESO   | ALMACENAMIENTO DE DOCUMENTOS   | COPIA O REPRODUCCIÓN  | TRASLADO DE DOCUMENTACIÓN                                      | GESTIÓN DE DOCUMENTOS Y SOPORTES   | CONTROL DE ACCESO  | TELECOMUNICACIONES  |
| 1. Acceso solo para personal autorizado.<br><br>2. Mecanismo de identificación de acceso.<br><br>3. Registro de accesos de usuarios no autorizados. | 1. Archivos, armarios u otros ubicados en áreas de acceso protegidas con llaves u otras medidas. | 1. Solo por usuarios autorizados.<br><br>2. Destrucción que impida el acceso o recuperación de los datos. | 1. Medidas que impidan el acceso o manipulación de documentos. | 1. Sistema de etiquetado confidencial.<br><br>2. Cifrado de datos.<br><br>3. Cifrado de dispositivos portátiles cuando salgan fuera. | 1. Registro de accesos: usuario, hora, base de datos a la que accede, tipo de acceso, registro al que accede.<br><br>2. Control del registro de accesos por el responsable de seguridad. Informe mensual.<br><br>3. Conservación de los datos: 2 años. | 1. Transmisión de datos mediante redes electrónicas cifradas. |

## 12. TRANSFERENCIA DE DATOS A TERCEROS PAÍSES

De acuerdo con el Título VIII de la LEPD, se prohíbe la transferencia de datos personales a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la LEPD exige a sus destinatarios. Esta prohibición no regirá cuando se trate de:



- Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.
- Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del Titular por razones de salud o higiene pública.
- Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.
- Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.
- Transferencias necesarias para la ejecución de un contrato entre el Titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.
- Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

En los casos no contemplados como excepción, corresponderá a la Superintendencia de Industria y Comercio proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. El Superintendente está facultado para requerir información y adelantar las diligencias tendentes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

Las transmisiones internacionales de datos personales que se efectúen entre un responsable y un encargado para permitir que el encargado realice el tratamiento por cuenta del responsable, no requerirán ser informadas al Titular ni contar con su consentimiento, siempre que exista un contrato de transmisión de datos personales."

### **13. VIGENCIA DE LA POLÍTICA Y LAS BASES DE DATOS**

Las bases de datos responsabilidad del **FONDO DE EMPLEADOS DE ORACLE**, serán objeto de tratamiento durante el tiempo que sea razonable y necesario para la finalidad para la cual son recabados los datos. Una vez



cumplida la finalidad o finalidades del tratamiento, y sin perjuicio de normas legales que dispongan lo contrario. El **FONDO DE EMPLEADOS DE ORACLE**, procederá a la supresión de los datos personales en su posesión salvo que exista una obligación legal o contractual que requiera su conservación.

De acuerdo con lo, dicha base de datos ha sido creada sin un periodo de vigencia definido. La presente política de tratamiento permanece vigente desde Junio de 2017 siendo actualizada cada año.

