MANUAL DE POLÍTICAS Y PROCEDIMIENTOS

Ley 1581 de 2012 de Protección de Datos Personales

Última actualización: marzo de 2026

FONDO DE EMPLEADOS DE ORACLE - FEORACLE

ÍNDICE

1.BASE LEGAL Y ÁMBITO DE APLICACIÓN

La presente Política de Tratamiento de la Información se desarrolla en estricto cumplimiento de los mandatos superiores previstos en los **artículos 15 y 20 de la Constitución Política de Colombi**a, así como en las disposiciones establecidas en la ***Ley Estatutaria 1581 de 2012 de Protección de Datos Personales*** y su normativa reglamentaria, especialmente el *Decreto 1377 de 2013 y el Decreto Único Reglamentario 1074 de 2015, junto con el Decreto 090 de 2018, el Decreto 255 de 2022* y las instrucciones impartidas por la Superintendencia de Industria y Comercio mediante la **Circular Externa 003 de 2018** y demás normas concordantes, complementarias o sustitutivas.

La presente política aplica a todos los datos personales tratados por el fondo de empleados de oracle – **feoracle,** en calidad de responsable del tratamiento, así como a los tratamientos realizados por terceros que actúen como Encargados por cuenta de la organización. Su alcance comprende la información de empleados, candidatos, clientes, proveedores, contratistas, aliados comerciales, visitantes y cualquier titular cuyos datos personales sean objeto de recolección, almacenamiento, uso, circulación, transmisión, transferencia o supresión, independientemente del medio utilizado o del lugar desde el cual se realice el tratamiento, siempre que este se encuentre sujeto a la legislación colombiana.

El tratamiento de datos personales se efectuará conforme a los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad, bajo el enfoque de responsabilidad demostrada que obliga al responsable del tratamiento a adoptar medidas que permitan evidenciar el cumplimiento de la normativa vigente.

Finalmente, el tratamiento de datos personales relacionados con riesgos de ***Lavado de Activos (LA), Financiación del Terrorismo (FT) y Proliferación de Armas de Destrucción Masiva (PADM)*** se realizará en cumplimiento de obligaciones legales y regulatorias aplicables, pudiendo efectuarse sin autorización del titular cuando exista mandato legal o requerimiento de autoridad competente, incluyendo el reporte ante la Unidad de Información y Análisis Financiero ***(UIAF)*** y demás autoridades de control, vigilancia o judiciales.

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

- Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.
- Base de datos: Conjunto organizado de datos personales que sea objeto de tratamiento.
- Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- Dato público: Es el dato que no 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 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.
- Dato semiprivado: Dato que no tiene naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector o grupo de personas, como la información financiera, crediticia o comercial.
- Dato privado: Dato que por su naturaleza íntima o reservada solo es relevante para el titular, como dirección personal, teléfono privado o información laboral no pública.
- 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.
- 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.
- Autorización inequívoca: Manifestación del titular mediante la cual se evidencia de forma razonable su consentimiento para el tratamiento de datos personales, incluyendo medios electrónicos o conductas que permitan concluir dicha autorización.
- Consulta: Solicitud del titular para conocer la información que repose en bases de datos.
  Reclamo: Solicitud del titular para corregir, actualizar, suprimir o revocar la autorización.
- 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.
- 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.

3. AUTORIZACIÓN DE LA POLÍTICA DE TRATAMIENTO

De conformidad con lo dispuesto en el artículo 9 de la Ley Estatutaria 1581 de 2012 y el Decreto 1377 de 2013, el tratamiento de datos personales por parte del fondo de empleados de oracle – **feoracle,** requiere la autorización previa, expresa e informada del Titular, la cual será obtenida a más tardar al momento de la recolección de los datos personales.

La aceptación de la presente Política de Tratamiento de la Información constituye un mecanismo de información al titular, pero no sustituye la autorización individual que debe otorgarse para el tratamiento de los datos personales conforme a las finalidades previamente informadas, podrá obtenerse mediante cualquier medio que permita su consulta posterior, incluyendo, entre otros:

- Documentos físicos firmados por el titular.
- Medios electrónicos o digitales, tales como formularios web, correos electrónicos o aceptación mediante casillas de verificación.
- Grabaciones de voz en procesos de atención telefónica o call center.
- Conductas inequívocas del titular que permitan concluir razonablemente que otorgó su consentimiento.

El fondo de empleados de oracle – **feoracle,** conservará prueba de la autorización otorgada por los titulares de los datos personales conforme a las obligaciones legales vigentes.

El Titular podrá revocar la autorización otorgada en cualquier momento y solicitar la supresión de sus datos personales, salvo cuando exista un deber legal o contractual que impida su eliminación.

3.1 Tratamiento de datos sensibles

Cuando el tratamiento involucre datos sensibles, el Titular será informado de manera previa y expresa que:

- No está obligado a autorizar el tratamiento de datos sensibles.
- La autorización es facultativa.
- Se indicarán claramente las finalidades específicas del tratamiento.

3.2 Tratamiento de datos de niños, niñas y adolescentes

El tratamiento de datos personales de niños, niñas y adolescentes se realizará únicamente cuando responda y respete su interés superior y asegure el respeto de sus derechos fundamentales. En tales casos, la autorización deberá ser otorgada por el representante legal del menor, previa verificación del cumplimiento de los requisitos legales aplicables.

3.4 Casos en los cuales no se requiere autorización

De conformidad con el artículo 10 de la Ley 1581 de 2012 de Protección de Datos personales, 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.
- Tratamientos necesarios para el cumplimiento de obligaciones legales relacionadas con la prevención y control del lavado de activos, financiación del terrorismo y proliferación de armas de destrucción masiva, cuando exista mandato legal o requerimiento de autoridad competente.

4. RESPONSABLE DEL TRATAMIENTO

El responsable del tratamiento de las bases de datos objeto de esta política es el fondo de empleados de oracle – **feoracle,** cuyos datos de contacto son los siguientes:

- Dirección: Calle 127 a 53ª - 45 Torre 2 de la ciudad de Bogotá D.C.
- Correo electrónico: https://www.feoracle.com.co/
- Teléfono: 6451051 -3587173 - 3209195668
- Página Web: https://www.feoracle.com.co

5. TRATAMIENTO Y FINALIDADES DE LAS BASES DE DATOS

Las finalidades descritas en la presente política corresponden a propósitos legítimos, específicos y previamente informados a los titulares de los datos personales, conforme al principio de finalidad establecido en la Ley 1581 de 2012.

Para efectos de transparencia y responsabilidad demostrada, el fondo de empleados de oracle – **feoracle,** clasifica las finalidades del tratamiento en:

- Finalidades principales: aquellas necesarias para el desarrollo de la relación contractual, legal o comercial con el titular y sin las cuales no sería posible ejecutar la relación correspondiente.
- Finalidades secundarias: aquellas adicionales que no son indispensables para la ejecución de la relación principal, tales como actividades de mercadeo, prospección comercial, invitaciones a eventos, estudios estadísticos o envío de información promocional, respecto de las cuales el titular podrá autorizar o no su tratamiento.

Asimismo, para cada base de datos se identifican los tipos de datos personales tratados y los periodos de conservación definidos conforme a obligaciones legales, contractuales y criterios de necesidad del tratamiento.

En los casos en que se traten datos sensibles, incluyendo datos biométricos obtenidos mediante sistemas de videovigilancia o mecanismos de control de acceso, el fondo de empleados de oracle – **feoracle,** garantizará el cumplimiento de las condiciones reforzadas de protección previstas en la legislación vigente, informando previamente al titular sobre la finalidad específica del tratamiento y el carácter facultativo de su autorización cuando esta sea requerida.

TABLA I. BASES DE DATOS Y FINALIDADES

BASE DE DATOS	TOPO DE DATOS	FINALIDADES PRIMARIAS	FINALIDADES SECUNDARIAS	TIEMPO DE CONSERVACION DE LOS DATOS
ASOCIADOS	**SENSIBLES**	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.	• Recursos Humanos – Control de horario • Recursos Humanos – Formación de personal • Recursos Humanos – Prestaciones sociales • Recursos Humanos – Prevención de riesgos laborales • Gestión contable, fiscal y administrativa - Gestión administrativa	7 años, siendo actualizada cada año.
PROVEEDORESY CONVENIOS	**PRIVADOS**	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.	• Gestión contable, fiscal y administrativa - Gestión de proveedores. • Gestión contable, fiscal y administrativa - Gestión administrativa	7 años, siendo actualizada cada año.
EMPLEADOS	**SENSIBLES**	Recolección, custodia, almacenamiento, tratamiento y de datos personales de empleados, hojas de vida, gestión de pagos, nomina, incapacidades, control de horario, delegación de funciones, historial laboral etc.	• Recursos humanos - Control de horario • Recursos humanos - Gestión de nómina. • Recursos humanos - Gestión de personal • Gestión contable, fiscal y administrativa - Gestión administrativa	7 años, siendo actualizada cada año.
DECSIS	**PRIVADOS**	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.	• Finalidades varias - Procedimientos administrativos •Recursos humanos - Control de horario • Seguridad - Seguridad y control de acceso a edificios.	7 años, siendo actualizada cada año.

El tratamiento de datos biométricos y sistemas de videovigilancia tiene como única finalidad la seguridad de personas, bienes e instalaciones, el control de acceso y la prevención de incidentes, y se realiza conforme a medidas reforzadas de seguridad y acceso restringido.

6. DERECHOS DE LOS TITULARES DE LOS DATOS PERSONALES

De conformidad con lo dispuesto en el artículo 8 de la Ley 1581 de 2012 (LEPD) y en 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 personales tratados por el fondo de empleados de oracle – **feoracle,** podrán ejercer los siguientes derechos respecto del tratamiento de su información personal.

6.1. Personas facultadas para ejercer los derechos

Los derechos de los Titulares podrán ejercerse por las siguientes personas:

- El Titular, quien deberá acreditar su identidad por los medios que disponga el responsable del tratamiento.
- Sus causahabientes, quienes deberán acreditar dicha calidad.
- El representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento correspondiente.
- Por estipulación a favor de otro o para otro, cuando resulte aplicable conforme a la ley.
- Los derechos de los niños, niñas y adolescentes serán ejercidos por las personas que se encuentren legalmente facultadas para su representación.

6.2. Derechos de los Titulares

El Titular de los datos personales tendrá los siguientes derechos:

6.2.1 Derecho de acceso o consulta

Conocer, previa solicitud, la existencia del tratamiento de sus datos personales, así como el origen, uso, finalidad y condiciones del tratamiento efectuado por el responsable.

6.2.2 Derecho a presentar consultas, quejas y reclamos

El Titular podrá presentar reclamos cuando considere que la información contenida en una base de datos debe ser objeto de corrección, actualización, supresión o cuando advierta el presunto incumplimiento de cualquiera de los deberes legales.

Los reclamos podrán clasificarse en:

Reclamo de corrección: Derecho a actualizar, rectificar o modificar datos parciales, inexactos, incompletos, fraccionados o que induzcan a error, o cuyo tratamiento esté prohibido o no autorizado.

Reclamo de supresión: Derecho a solicitar la eliminación de los datos cuando resulten inadecuados, excesivos o cuando el tratamiento no respete los principios, derechos y garantías constitucionales y legales.

Reclamo de revocación: Derecho a revocar la autorización otorgada para el tratamiento de datos personales, salvo cuando exista un deber legal o contractual que impida su eliminación.

Reclamo por infracción: Derecho a solicitar la corrección de situaciones que impliquen incumplimiento de la normativa de protección de datos personales.

6.2.3 Derecho a solicitar prueba de la autorización

Solicitar prueba de la autorización otorgada al responsable del tratamiento, salvo en los casos expresamente exceptuados por la ley, de conformidad con el artículo 10 de la Ley 1581 de 2012.

6.2.4 Derecho a presentar quejas ante la Superintendencia de Industria y Comercio

Presentar quejas ante la Superintendencia de Industria y Comercio por infracciones a la normativa de protección de datos personales, una vez se haya agotado el trámite de consulta o reclamo ante el responsable o encargado del tratamiento.

El fondo de empleados de oracle – **feoracle,**. garantizará mecanismos sencillos, gratuitos y accesibles para el ejercicio de los derechos aquí descritos.

7. ATENCIÓN A LOS TITULARES DE DATOS – OFICIAL DE CUMPLIMIENTO

Giovanny Antonio Melo Piramanrique del fondo de empleados de oracle – **feoracle,** será el encargado de la atención de peticiones, consultas y reclamos ante la cual el Titular de los datos puede ejercer sus derechos. Teléfono: 6451051 -3587173 - 3209195668, correo electrónico: riesgos@feoracle.com.co.

8. PROCEDIMIENTOS PARA EL EJERCICIO DE LOS DERECHOS DEL TITULAR

El fondo de empleados de oracle – **feoracle,** garantiza a los Titulares el ejercicio efectivo de sus derechos mediante procedimientos sencillos, gratuitos y accesibles, conforme a lo dispuesto en los artículos 14 y 15 de la Ley 1581 de 2012 y el Capítulo 25 del Decreto 1074 de 2015.

8.1 Derecho de acceso o consulta

De acuerdo con el artículo 2.2.2.25.4.2 del Decreto 1074 de 2015, el Titular o sus causahabientes podrán consultar gratuitamente sus datos personales:

- Al menos una (1) vez cada mes calendario.
- Cada vez que existan modificaciones sustanciales en las políticas de tratamiento de la información que motiven nuevas consultas.

Para consultas cuya periodicidad sea superior a una por mes calendario, el fondo de empleados de oracle – **feoracle,** podrá cobrar únicamente los gastos de envío, reproducción y certificación de documentos, los cuales no podrán superar los costos de recuperación del material correspondiente. Dichos costos deberán ser demostrables ante la Superintendencia de Industria y Comercio cuando esta lo requiera.

Canales para presentar consultas

- El Titular podrá ejercer este derecho mediante solicitud dirigida a el fondo de empleados de oracle – **feoracle,** a través de:

- Correo electrónico: riesgos@feoracle.com.co.
- Correo físico Calle 127 a 53ª - 45 Torre 2 de la ciudad de Bogotá D.C.
- Indicando en el asunto: “Consulta de datos personales”.

La solicitud deberá contener como mínimo:

- Nombre completo del Titular.
- Copia del documento de identidad del Titular o de su representante.
- Descripción clara de la consulta.
- Dirección física o electrónica para recibir respuesta.
- Fecha y firma del solicitante.
- Documentos soporte cuando resulte aplicable.
- Medios de respuesta

El Titular podrá recibir la información mediante:

- Visualización electrónica.
- Copia física enviada por correo.
- Correo electrónico u otro medio digital.
- Cualquier otro mecanismo técnicamente disponible según la naturaleza del tratamiento.

Término de respuesta

El fondo de empleados de oracle – **feoracle,** responderá la consulta en un término máximo de diez (10) días hábiles contados desde la fecha de recibo.

Si no fuere posible atenderla dentro de dicho término, se informará al interesado antes de su vencimiento, indicando los motivos de la demora y la nueva fecha de respuesta, la cual no podrá superar cinco (5) días hábiles adicionales.

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

8.2 Procedimiento para quejas y reclamos

El Titular o sus causahabientes podrán presentar reclamos cuando consideren que la información contenida en una base de datos debe ser objeto de:

- Corrección
- Actualización
- Supresión
- Revocatoria de autorización o cuando adviertan incumplimiento de la normativa de protección de datos personales.
- Canales de recepción

Las solicitudes deberán enviarse a:

- Correo electrónico: riesgos@feoracle.com.co.

- Dirección física: Calle 127 a 53ª - 45 Torre 2 de la ciudad de Bogotá D.C.
- Indicando en el asunto: “Reclamo de protección de datos personales”.
- Información mínima del reclamo
- El reclamo deberá contener:
- Nombre completo del Titular.
- Copia del documento de identidad.
- Descripción de los hechos y solicitud concreta.
- Dirección de notificación.
- Fecha y firma del solicitante.
- Documentos soporte cuando corresponda.

Reclamo incompleto

Si el reclamo se encuentra incompleto, el fondo de empleados de oracle – **feoracle,** requerirá al interesado dentro de los cinco (5) días hábiles siguientes para subsanar la información.

Si transcurren dos (2) meses sin respuesta, se entenderá que el solicitante ha desistido del reclamo.

Registro del reclamo

Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que indique:

“Reclamo en trámite”, junto con el motivo del mismo, en un plazo máximo de dos (2) días hábiles.

Dicha leyenda permanecerá hasta que el reclamo sea resuelto.

Término de respuesta

El reclamo será atendido en un término máximo de quince (15) días hábiles contados a partir del día siguiente a su recepción.

Cuando no sea posible resolverlo dentro del término inicial, se informará al interesado antes de su vencimiento indicando los motivos de la demora y la nueva fecha de respuesta, la cual no podrá superar ocho (8) días hábiles adicionales.

Una vez agotado el trámite interno, el Titular podrá presentar queja ante la Superintendencia de Industria y Comercio.

El fondo de empleados de oracle – **feoracle,** dejará constancia de la recepción y trámite de todas las consultas y reclamos presentados por los Titulares, garantizando la trazabilidad del proceso y el cumplimiento de los principios de transparencia y responsabilidad demostrada.

9. MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN

El fondo de empleados de oracle – **feoracle,** en cumplimiento del principio de seguridad consagrado en el artículo 4 literal g) de la Ley 1581 de 2012 y las disposiciones del Decreto 1074 de 2015, ha adoptado medidas técnicas, humanas y administrativas necesarias para proteger los datos personales objeto de tratamiento, evitando su adulteración, pérdida, consulta, uso, acceso o reproducción no autorizada o fraudulenta.

Las medidas implementadas buscan garantizar la confidencialidad, integridad, disponibilidad y resiliencia de la información personal tratada por la organización, conforme al principio de responsabilidad demostrada.

9.1. Medidas administrativas

El fondo de empleados de oracle – **feoracle,** ha implementado, entre otras, las siguientes medidas administrativas:

- Adopción de la presente Política de Tratamiento de Datos Personales.
- Designación de responsables internos para la gestión de protección de datos personales.
- Implementación de procedimientos para el ejercicio de derechos de los Titulares.
- Suscripción de acuerdos de confidencialidad con empleados, contratistas y terceros.
- Control documental y gestión de autorizaciones de tratamiento.
- Evaluación periódica del cumplimiento normativo en materia de protección de datos.

9.2. Medidas técnicas

La organización ha adoptado controles tecnológicos orientados a prevenir accesos no autorizados y proteger la información, tales como:

- Control de acceso a sistemas de información mediante credenciales individuales.
- Uso de mecanismos de autenticación y perfiles de usuario.
- Protección perimetral y monitoreo de redes y equipos.
- Copias de seguridad periódicas y mecanismos de recuperación de información.
- Sistemas de almacenamiento seguro y control de accesos a bases de datos.
- Implementación de medidas de seguridad para datos biométricos y videovigilancia.

9.3. Medidas humanas

El fondo de empleados de oracle – **feoracle,** promueve la protección de datos personales mediante:

- Capacitación periódica del personal en protección de datos y seguridad de la información.
- Deber de confidencialidad para todos los colaboradores.

- Restricción del acceso a la información conforme al principio de necesidad y finalidad.
- Procedimientos disciplinarios frente al uso indebido de la información.

9.4. Medidas aplicables a encargados del tratamiento

Mediante la suscripción de contratos de transmisión y acuerdos de tratamiento de datos personales, el fondo de empleados de oracle – **feoracle,** exige a los encargados del tratamiento:

- Implementar medidas de seguridad equivalentes o superiores a las adoptadas por la organización.
- Garantizar la confidencialidad de la información.
- Tratar los datos únicamente conforme a las instrucciones del Responsable.
- Reportar incidentes de seguridad que comprometan datos personales.

9.5. Gestión de incidentes de seguridad

El fondo de empleados de oracle – **feoracle,** cuenta con procedimientos internos para la identificación, atención, mitigación y reporte de incidentes de seguridad que puedan afectar datos personales, incluyendo la evaluación del riesgo y, cuando corresponda, la notificación a la Superintendencia de Industria y Comercio y a los Titulares afectados.

9.6. Actualización y mejora continua

Las medidas de seguridad serán revisadas y actualizadas periódicamente conforme a:

- Cambios regulatorios.
- Evolución tecnológica.
- Identificación de nuevos riesgos.
- Resultados de auditorías internas o externas.

Las medidas aquí descritas se encuentran desarrolladas de manera detallada en el Manual Interno de Seguridad de la Información del fondo de empleados de oracle – **feoracle,** el cual contiene las Tablas II, III, IV y V correspondientes a los controles específicos implementados por la organización.

10. DEBERES DEL RESPONSABLE, ENCARGADOS Y PERSONAS AUTORIZADAS PARA EL TRATAMIENTO DE DATOS PERSONALES

El fondo de empleados de oracle – **feoracle,** en calidad de Responsable del Tratamiento, así como los encargados, empleados, contratistas y terceros que actúen en su nombre y representación y que tengan acceso a datos personales, deberán observar y cumplir las disposiciones contenidas en la presente Política de Tratamiento de Datos Personales durante el desarrollo de sus funciones y aun después de finalizados los vínculos legales, comerciales, contractuales o laborales que dieron origen al tratamiento.

Todas las personas autorizadas para tratar datos personales deberán guardar estricta confidencialidad respecto de la información a la que tengan acceso.

10.1. Deberes del Responsable del Tratamiento

En cumplimiento del artículo 17 de la Ley 1581 de 2012, el fondo de empleados de oracle – **feoracle,** se compromete a:

- Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- Solicitar y conservar, en las condiciones previstas por la ley, copia de la autorización otorgada por el Titular.
- Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten.
- 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 suministrada al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- Actualizar la información y comunicar oportunamente al Encargado del Tratamiento todas las novedades respecto de los datos previamente suministrados.
- Rectificar la información cuando sea incorrecta e informar lo pertinente al Encargado del Tratamiento.
- Suministrar únicamente datos cuyo tratamiento esté previamente autorizado conforme a la ley.
- Exigir al Encargado del Tratamiento el respeto permanente de las condiciones de seguridad y privacidad de la información.
- Tramitar las consultas y reclamos formulados por los Titulares en los términos legales.
- Adoptar políticas y procedimientos internos que garanticen el cumplimiento de la normativa de protección de datos personales.
- Informar al Encargado del Tratamiento cuando determinada información se encuentre en discusión por parte del Titular.
- Informar al Titular, cuando este lo solicite, sobre el uso dado a sus datos personales.
- Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad que impliquen riesgos en la administración de la información.
- Cumplir las instrucciones y requerimientos impartidos por la Superintendencia de Industria y Comercio.

10.2. Deberes de los Encargados del Tratamiento

Los Encargados del Tratamiento que actúen por cuenta del fondo de empleados de oracle – **feoracle,** deberán cumplir las obligaciones establecidas en el artículo 18 de la Ley 1581 de 2012, incluyendo:

Tratar los datos personales únicamente conforme a las instrucciones del Responsable.

Salvaguardar la seguridad de las bases de datos.

Mantener la confidencialidad de la información.

Garantizar el ejercicio de los derechos de los Titulares.

Informar incidentes de seguridad que comprometan datos personales.

10.3. Deber de confidencialidad

El fondo de empleados de oracle – **feoracle,** tratará como información confidencial todos los datos personales recolectados y almacenados en sus bases de datos, independientemente del medio en que se encuentren. Para garantizar lo anterior, la organización:

Suscribirá acuerdos de confidencialidad con empleados, contratistas y terceros autorizados.

Implementará controles de acceso y medidas de protección de la información conforme a sus políticas internas de seguridad.

Exigirá a los receptores de datos personales, en casos de transmisión o transferencia de información, el cumplimiento de obligaciones equivalentes de confidencialidad y seguridad.

El deber de confidencialidad subsistirá aun después de finalizada la relación contractual, laboral o comercial con el fondo de empleados de oracle – **feoracle**.

11. MECANISMOS DE DIVULGACIÓN Y ACCESO A LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

El fondo de empleados de oracle – **feoracle,** garantiza a los Titulares el acceso permanente, gratuito y fácil a la presente Política de Tratamiento de Datos Personales, en cumplimiento del principio de transparencia establecido en la Ley 1581 de 2012.

La política podrá ser consultada a través de los siguientes canales oficiales:

- **Página web institucional:** https://www.feoracle.com.co
- **Correo electrónico:** riesgos@feoracle.com.co.

Los Titulares podrán solicitar en cualquier momento copia de la Política de Tratamiento de Datos Personales mediante solicitud enviada al correo electrónico indicado, la cual será suministrada sin costo alguno.

El fondo de empleados de oracle – **feoracle,** mantendrá la versión vigente de esta política publicada y disponible para consulta pública, garantizando su actualización cuando se presenten modificaciones sustanciales en el tratamiento de datos personales.

12. MECANISMOS DE RECOLECCIÓN DE DATOS PERSONALES Y DEBER DE INFORMACIÓN

El fondo de empleados de oracle – **feoracle,** realiza la recolección de datos personales mediante mecanismos físicos y digitales, garantizando en todo momento el cumplimiento de los principios de legalidad, libertad, transparencia y finalidad establecidos en la Ley 1581 de 2012.

La recolección de datos personales se lleva a cabo a través de:

- Formularios físicos bajo la modalidad de contacto cero con el Titular.
- Formularios digitales disponibles en la página web institucional y demás canales electrónicos autorizados.

En cada uno de los mecanismos de recolección, el fondo de empleados de oracle – **feoracle,** informa previamente al Titular, de manera clara y expresa:

- La identidad y datos de contacto del Responsable del Tratamiento.
- Las finalidades específicas para las cuales se recolectan los datos personales.
- Los derechos que le asisten como Titular de la información.
- Los canales habilitados para el ejercicio de dichos derechos.
- Los medios a través de los cuales puede consultar la Política de Tratamiento de Datos Personales.

Lo anterior se realiza mediante la puesta a disposición del correspondiente **Aviso de Privacidad**, garantizando que la autorización otorgada por el Titular sea previa, expresa e informada, conforme a los artículos 9 y 12 de la Ley 1581 de 2012.

El fondo de empleados de oracle – **feoracle,** conserva evidencia de las autorizaciones otorgadas por los Titulares y de los mecanismos utilizados para el suministro de la información requerida por la normativa vigente.

13. TRANSFERENCIA Y TRANSMISIÓN NACIONAL E INTERNACIONAL DE DATOS PERSONALES

El fondo de empleados de oracle – **feoracle,** podrá realizar transferencia y transmisión de datos personales a terceros ubicados dentro o fuera del territorio nacional, en cumplimiento de lo dispuesto en el Título VIII de la Ley 1581 de 2012 y el Decreto 1074 de 2015, garantizando en todo momento la protección de los derechos de los Titulares.

13.1. Transferencia internacional de datos personales

Se entiende por transferencia el envío de datos personales por parte del fondo de empleados de oracle – **feoracle,** en calidad de Responsable del Tratamiento, a otro Responsable ubicado en Colombia o en el extranjero.

De conformidad con la normativa vigente, se prohíbe la transferencia de datos personales a países que no proporcionen niveles adecuados de protección de datos personales.

Un país se considerará con nivel adecuado de protección cuando cumpla los estándares establecidos por la Superintendencia de Industria y Comercio, los cuales no podrán ser inferiores a los exigidos por la Ley 1581 de 2012.

13.2. Excepciones a la prohibición de transferencia internacional

La prohibición anterior no aplicará cuando:

- El Titular haya otorgado autorización previa, expresa e inequívoca para la transferencia.
- El intercambio de datos médicos sea requerido para el tratamiento del Titular por razones de salud o higiene pública.
- Se trate de transferencias bancarias o bursátiles conforme a la legislación aplicable.
- La transferencia se realice en el marco de tratados internacionales suscritos por la República de Colombia bajo el principio de reciprocidad.
- Sea necesaria para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales con autorización del Titular.
- Sea legalmente exigida para la salvaguardia del interés público o para el reconocimiento, ejercicio o defensa de un derecho dentro de un proceso judicial.
- En los casos que no se encuentren dentro de las excepciones previstas, corresponderá a la Superintendencia de Industria y Comercio emitir la declaración de conformidad para la transferencia internacional de datos personales.

13.3. Transmisión nacional o internacional de datos personales

Se entiende por transmisión el tratamiento de datos personales que implica la comunicación de los mismos a un Encargado del Tratamiento, dentro o fuera de Colombia, para que realice el tratamiento por cuenta del fondo de empleados de oracle – **feoracle**.

Las transmisiones de datos personales no requieren una nueva autorización del Titular cuando:

- El tratamiento se encuentre dentro de las finalidades previamente autorizadas.
- Exista un contrato de transmisión de datos personales conforme al artículo 2.2.2.25.5.2 del Decreto 1074 de 2015.
- Dicho contrato deberá establecer, como mínimo:
- El alcance del tratamiento.
- Las actividades que el Encargado realizará por cuenta del Responsable.
- Las obligaciones de confidencialidad.
- Las medidas de seguridad aplicables.
- La prohibición de uso de la información para fines distintos.
- El deber de atender consultas y reclamos conforme a la ley.

13.4. Garantías de protección

El fondo de empleados de oracle – **feoracle,** adoptará las medidas necesarias para verificar que los terceros receptores de datos personales, nacionales o internacionales garanticen condiciones adecuadas de seguridad, confidencialidad y protección de la información, conforme al principio de responsabilidad demostrada.

En todos los casos se asegurará que el tratamiento de los datos personales se limite a las finalidades autorizadas por el Titular y al cumplimiento de obligaciones legales o contractuales aplicables.

14. MODIFICACIÓN Y/O ACTUALIZACIÓN DE LA POLÍTICA

El fondo de empleados de oracle – **feoracle,** informará cualquier cambio sustancial que pueda existir en la presente política y las diferentes medidas de seguridad, de manera que comunicará de forma oportuna a los Titulares de los datos a través de la página web https://www.feoracle.com.co o cuando corresponda mediante correo electrónico masivo.

15. VIGENCIA DE LA POLÍTICA Y PERÍODO DE CONSERVACIÓN DE LOS DATOS PERSONALES

15.1. Vigencia de la Política de Tratamiento de Datos Personales

La presente Política de Tratamiento de Datos Personales del fondo de empleados de oracle – **feoracle,** rige a partir de su fecha de publicación y permanecerá vigente mientras la organización realice el tratamiento de datos personales y/o mientras subsistan las finalidades que dieron origen a su recolección.

El fondo de empleados de oracle – **feoracle,** se reserva el derecho de modificar o actualizar esta política en cualquier momento, con el fin de adaptarla a cambios legislativos, regulatorios, jurisprudenciales, tecnológicos o internos de la organización.

Cualquier modificación sustancial será informada oportunamente a los Titulares mediante la publicación de la versión actualizada en la página web institucional.

15.2. Período de conservación de los datos personales

- Los datos personales tratados por el fondo de empleados de oracle – **feoracle,** serán conservados únicamente durante el tiempo que resulte necesario para cumplir con las finalidades para las
  cuales fueron recolectados, así como para atender obligaciones legales, contractuales, contables, fiscales, laborales o administrativas aplicables.
- Una vez cumplida la finalidad del tratamiento y siempre que no exista un deber legal o contractual que requiera su conservación, los datos personales serán eliminados, anonimizados o bloqueados de forma segura.

15.3. Criterios generales de conservación

El fondo de empleados de oracle – **feoracle,** aplicará los siguientes criterios para determinar los períodos de conservación:

- Vigencia de la relación contractual, comercial o laboral con el Titular.
- Cumplimiento de obligaciones legales o regulatorias.
- Términos de prescripción legal aplicables.
- Necesidades probatorias frente a autoridades administrativas o judiciales.
- Finalidades históricas, estadísticas o científicas cuando sea procedente.

15.4. Tiempos estimados de conservación por tipo de base de datos

De manera general, los datos personales serán conservados conforme a los siguientes períodos orientativos:

- Datos de empleados y exempleados: durante la relación laboral y hasta veinte (20) años posteriores, conforme a obligaciones laborales y de seguridad social.
- Hojas de vida: hasta dos (2) años después de finalizado el proceso de selección, salvo autorización para conservación futura.
- Clientes y proveedores: durante la vigencia de la relación contractual y hasta diez (10) años adicionales conforme a obligaciones contables y fiscales.
- Datos comerciales y de mercadeo: hasta que el Titular solicite la supresión o revoque la autorización.
- Registros de videovigilancia y biometría: por un período máximo de noventa (90) días, salvo requerimiento de autoridad competente o necesidad probatoria.
- Datos recolectados en eventos y campañas comerciales: hasta cinco (5) años o hasta la revocatoria de la autorización por parte del Titular.

15.5. Supresión de la información

El Titular podrá solicitar en cualquier momento la supresión de sus datos personales cuando:

- No se respeten los principios, derechos y garantías constitucionales y legales.
- Los datos hayan dejado de ser necesarios para la finalidad para la cual fueron recolectados.
- Se haya revocado la autorización, siempre que no exista un deber legal o contractual que impida su eliminación.
- El fondo de empleados de oracle – **feoracle,** procederá a la supresión segura de los datos personales conforme a los procedimientos internos de gestión de la información y seguridad establecidos por la organización.

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
1. Medidas que eviten el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruidos. 2. Acceso restringido al lugar donde se almacenan los datos. 3. Autorización del responsable para la salida de documentos o soportes por medio físico o electrónico. 4. Sistema de etiquetado o identificación del tipo de información. 5. Inventario de soportes.	1. Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones. 2. Lista actualizada de usuarios y accesos autorizados. 3. Mecanismos para evitar el acceso a datos con derechos distintos de los autorizados. 4. Concesión, alteración o anulación de permisos por el personal autorizado	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. 2. Procedimiento de notificación y gestión de incidencias.	1. Definición de las funciones y obligaciones de los usuarios con acceso a los datos 2. Definición de las funciones de control y autorizaciones delegadas por el responsable del tratamiento. 3. Divulgación entre el personal de las normas y de las consecuencias del incumplimiento de las mismas	1. Elaboración e implementación del Manual de obligatorio cumplimiento para el personal. 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.

TABLA III. 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. 2. Auditoría extraordinaria por modificaciones sustanciales en los sistemas de información. 3. Informe de detección de deficiencias y propuesta de correcciones. 4. Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento. 5. Conservación del Informe a disposición de la autoridad.	1. Designación de uno o varios responsables de seguridad. 2. Designación de uno o varios encargados del control y la coordinación de las medidas del Manual Interno de Seguridad. 3. Prohibición de delegación de la responsabilidad del responsable del tratamiento en el responsable de seguridad.	1. Controles periódicos de cumplimiento	1. Registro de entrada y salida de documentos y soportes: fecha, emisor y receptor, número, tipo de información, forma de envío, responsable de la recepción o entrega.	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. Autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación.

TABLA IV. 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. 2. Mecanismos de identificación y autenticación; Contraseñas: asignación, caducidad y almacenamiento cifrado.	1. Acceso a datos mediante redes seguras.

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. 2. Mecanismo de identificación de acceso. 3. Registro de accesos de usuarios no autorizados.	1. Archivadores, armarios u otros ubicados en áreas de acceso protegidas con llaves u otras medidas.	1. Solo por usuarios autorizados. 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. 2. Cifrado de datos. 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. 2. Control del registro de accesos por el responsable de seguridad. Informe mensual. 3. Conservación de los datos: 2 años.	1. Transmisión de datos mediante redes electrónicas cifradas.