| PROTELA | POLÍTICA | | | |
|---|---|---|---|---|
| | POLÍTICA INTEGRAL DE GESTIÓN DE DATOS PERSONALES DE PROTELA S.A. | | | |
| CÓDIGO: TH-0048-POL-0112 | GESTIÓN JURÍDICA | | | |
| VERSIÓN: 2 | FECHA DE ACTUALIZACIÓN | 05 | 10 | 2023 |

## 1. Objetivo

Garantizar el cumplimiento de la normatividad vigente de habeas data, que señala los deberes del responsable o encargado del tratamiento de datos personales, entre los que se encuentra implementar políticas y procedimientos para la atención de consultas y reclamos sobre los datos recolectados, así como para su efectivo tratamiento.

## 2. Alcance

La Política Integral de Gestión de Datos Personales de PROTELA S.A. (en adelante Protela) aplica a todos los trabajadores, contratistas, proveedores, clientes, visitantes y a toda persona que se vea involucrada directa o indirectamente durante el desarrollo de las actividades en cada una de las dependencias que la conforman o que permanezcan en las instalaciones de la compañía, los cuales tengan datos personales registrados en cualquier base de datos de la empresa. Esta política es transversal a toda la operación de Protela y aplica para todas sus filiales.

## 3. Marco Normativo Externo

La ley 1581 de 2012 desarrolló el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Este derecho constitucional conocido como habeas data, confiere a los ciudadanos la posibilidad de decidir y controlar la información que otros poseen sobre ellos y, en ese orden de ideas, la ley 1581 de 2012 consagra mecanismos y garantías que permiten el pleno ejercicio del mencionado derecho.

En cumplimiento a lo establecido en la Ley 1266 de 2008, Ley 1581 de 2012, Decreto 1377 de 2013, el Decreto Único 1074 de 2015 en su capítulo 25 y las circulares de la Superintendencia de Industria y Comercio, Protela, en calidad de responsable del tratamiento de los datos personales de sus clientes, proveedores y colaboradores y encargado de algunas bases de datos de las empresas vinculadas, ha adoptado el presente programa integral de bases de datos para garantizar que la recolección y tratamiento de datos personales que hace se ajuste las disposiciones legales vigentes y cumpla con el principio de responsabilidad demostrada.

**1. NORMAS NACIONALES .**

. CONSTITUCIÓN POLÍTICA: Artículos 15 Y 20.

. LEYES: Ley 1266 de 2008, Ley 1581 de 2012.
. DECRETOS: Decreto 1074 de 2015, Decreto 1377 de 2013.
. CIRCULARES: Circular Externa 006 de 2022, Circular Única de la SIC, Título V.

**2. NORMAS Y ESTÁNDARES INTERNACIONALES.**

. RESOLUCIÓN 45/95 DE 1990 - ONU: Lista básica de principios para la protección de datos personales de aplicación mundial.

**3. REGLAMENTO INTERNO DE TRABAJO.**

. ARTÍCULO 43. OBLIGACIONES ESPECIALES DEL TRABAJADOR. Numeral 2. "No comunicar a terceros, salvo autorización expresa, las informaciones que sean de naturaleza reservada y cuya divulgación pueda ocasionar perjuicios a la empresa, lo que no obsta para denunciar delitos comunes o violaciones del contrato o de las normas legales de trabajo ante las autoridades competentes".

. ARTÍCULO 44. OBLIGACIONES ESPECIALES DEL TRABAJADOR. Numeral 11. "Guardar completa reserva sobre las operaciones, negocios y procedimientos industriales y comerciales, o cualquier otra clase de datos acerca de la Empresa que conozca por razón de sus funciones o de sus relaciones con la misma". Numeral 28. "Guardar estricta reserva sobre los hechos, documentos físicos y/o electrónicos, y de toda información que llegue a su conocimiento, por causa o con ocasión del ejercicio de la labor para la cual fue contratado, los cuales no podrán ser comunicados a terceros, salvo autorización expresa del empleador, cuando dicha información tenga naturaleza reservada y su divulgación pueda ocasionar perjuicios a la empresa".

. CAPÍTULO XXIII. PROTECCIÓN DE DATOS. ARTÍCULOS 95 Y 96.

## 4. Definiciones

**4.1. Autorización:** Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales;
**4.2. Aviso de privacidad:** Documento físico, electrónico o en cualquier otro formato, generado por el responsable, que es puesto a disposición del titular para el tratamiento de sus datos personales, el cual comunica al titular la información relativa a la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las características del Tratamiento que se pretende dar a los datos personales.
**4.3. Base de Datos:** Conjunto organizado de datos personales que sea objeto de tratamiento;
**4.4. Causahabiente:** Persona que es sucesora o heredera del Titular de la información a causa del fallecimiento de este.
**4.5. Confidencialidad:** Acceso a la información por parte únicamente de quienes estén autorizados, característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.
**4.6. Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;
**4.7. Dato privado:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.
**4.8. Dato semiprivado:** Aquel que no tiene naturaleza íntima, reservada, ni pública. Su conocimiento o divulgación puede interesar no solo al titular sino a un sector o grupo de personas o a la sociedad en general; tienen esta naturaleza los datos financieros, los crediticios, los relacionados con la actividad comercial o de servicios, entre otros.
**4.9. Dato sensible:** Aquel que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación, incluyendo pero sin limitarse a datos 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.
**4.10. 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
**4.11. Fuente de información:** Persona natural o jurídica que recibe o conoce datos personales del Titular, en virtud de una relación comercial, de servicio o de cualquier otra índole. Mediante autorización legal o del Titular puede transmitir o transferir estos datos a un responsable o encargado para su Tratamiento. Puede tener múltiples roles en el manejo de la información y ser al mismo tiempo responsable o encargado del Tratamiento.
**4.12. Habeas data:** Derecho de cualquier persona a conocer, actualizar y rectificar los datos o la información que se hayan recogido sobre ella en un banco de datos o en archivos de entidades públicas y privadas.
**4.13. Oficial de protección de datos:** Es la persona dentro de la empresa que tiene como función la vigilancia y control de la aplicación de la política de protección de datos.
**4.14. Principio de Territorialidad de la Ley Penal:** Se entiende como la posibilidad de que un Estado aplique las normas de su ordenamiento dentro del territorio bajo su dominio, sin interferencia alguna de otros Estados.
**4.15. Registro Nacional de Bases de Datos:** Es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país. El registro es administrado por la Superintendencia de Industria y Comercio y es de libre consulta para los ciudadanos.
**4.16. 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
**4.17. Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento
**4.18. Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

## 5. Responsabilidades

**5.1.** **PROTELA.**

En calidad de responsable o encargado del tratamiento de los datos personales, Protela acepta y reconoce que estos pertenecen única y exclusivamente a sus titulares y que sólo ellos pueden disponer sobre los mismos, razón por la cual, la compañía sólo hará uso de estos respetando la legislación vigente existente. Protela se compromete a cumplir con los siguientes deberes:

. Garantizar al titular de la información, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

. Conservar copia de la respectiva autorización otorgada por el titular.

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

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

. Actualizar la información y demás novedades respecto de los datos que previamente se hayan suministrado y adoptar las demás medidas necesarias para que la información suministrada a esta se mantenga actualizada.

. Rectificar la información cuando sea incorrecta.

. Tramitar las consultas y reclamos formulados por los titulares de la información en los términos señalados por los artículos 14 y 15 de la ley 1581 de 2012.

. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de Ley 1581 de 2012 y en especial, para la atención de consultas y reclamos.

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

. Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

. 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 o detalles del dato personal.

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

. Permitir el acceso a la información únicamente a las personas naturales o jurídicas que pueden tener acceso a ella.

. Informar a través de su página web los nuevos mecanismos que implemente para que los titulares de la información hagan efectivos sus derechos.

. Protela actualizará en el Registro Nacional de Bases de Datos la información registrada en sus Bases de datos dentro de los primeros diez (10) días hábiles de cada mes cuando se realicen cambios sustanciales en la información registrada, y anualmente independiente de si hay o no novedades entre el dos (2) de enero y el treinta y uno (31) de marzo de cada año. Adicionalmente, dentro de los quince (15) primeros días hábiles de los meses de febrero y agosto de cada año, Protela actualizará la información de los reclamos presentados.

**5.2. OFICIAL DE PROTECCIÓN DE DATOS.**

Será la persona que ejerza la vigilancia y control de la aplicación del programa integral de gestión de protección de datos personales dentro de la empresa. Este Oficial de Protección de Datos es el mismo Oficial de Cumplimiento designado por la Junta Directiva de Protela.

**Nombramiento:** El representante legal presentará la hoja de vida del oficial de protección de datos a la Junta Directiva para que esta apruebe o impruebe su nombramiento, bajo previa verificación de cumplimiento del perfil. Dicho nombramiento quedará consignado en el acta correspondiente de la reunión de Junta Directiva.
El nombramiento será por tiempo indefinido hasta su revocatoria, sustitución o retiro del trabajador de la Compañía.

**Auditorías y Supervisión:** El Oficial de Protección de Datos Personales podrá, en cualquier momento, ordenar auditorías de supervisión de cumplimiento de las disposiciones sobre protección de datos personales, con el propósito de garantizar el adecuado cumplimiento y desarrollo de la política de Protela. Como resultado de las revisiones pueden levantarse planes de acción para cerrar las brechas encontradas, los cuales tendrán seguimiento.

En todo caso, se realizará una auditoría interna anual para verificar el cumplimiento de las políticas por parte de Protela. Subcontratación: En el caso que Protela deba subcontratar a un tercero para realizar el tratamiento de datos, deberá suscribir los acuerdos de confidencialidad y alcance de tratamiento de los datos personales compartidos, siempre y cuando el titular haya autorizado dicha labor. El oficial de datos supervisará de forma exhaustiva dicho proceso.

**Designación:** Protela designa al oficial de cumplimiento, para cumplir con la función de protección de datos personales, así como para dar trámite a las solicitudes de los titulares, para el ejercicio de los derechos de acceso, consulta, rectificación, actualización, supresión y revocatoria a que se refiere la Ley 1581 de 2012.

De igual, manera la Junta Directiva designará el oficial de tratamiento de datos personales pudiendo ser el jefe jurídico u otra persona con las calidades establecidas en el presente documento.

El oficial de protección de datos deberá cumplir con los siguientes deberes y funciones:

. Verificar que la información se conserve bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

. Realizar oportunamente la actualización, rectificación o supresión de los datos.

. Tramitar las consultas y los reclamos del titular de los datos.

. Velar que el acceso a la información únicamente se realice por parte del personal autorizado o encargado.

. 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.

. Realizar las actualizaciones y reportes que solicite la Superintendencia de Industria y Comercio sobre las bases de datos que estén inscritas en el registro nacional de bases de Datos (RNBD).

. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

. Rendir mínimo un informe al año a la Junta Directiva donde se comuniquen las novedades presentadas y todo lo pertinente a la política de tratamiento de datos personales.
. Planear, ejecutar y seguir los elementos que hacen parte del programa integral de gestión de datos personales.

. Asesorar y sensibilizar a los empleados de la Compañía en relación con el programa y las principales obligaciones en su ejecución y desarrollo.

. Emitir conceptos y dar respuesta a las inquietudes y requerimientos sobre protección de datos personales a nivel interno y externo, así como asesorar sobre los asuntos relacionados con el manejo de información personal.

. Realizar el seguimiento de las normas sobre protección de datos personales y realizar las adecuaciones pertinentes al programa integral de gestión para procurar su cumplimiento.

. Gestionar y liderar el proceso de actualización de bases de datos ante el Registro Nacional de Bases de Datos y realizar los reportes legales que los entes de control soliciten.

. Coordinar los programas de capacitación y reinducción sobre el programa integral de gestión de datos personales.

. Revisar las actividades que generan algún tipo de tratamiento de los datos personales.

. Validar los puntos de captura de información personal, identificando el tipo de información que se recolecta y sus finalidades.

. Velar por la realización del inventario y actualización de las bases de datos identificadas.

. Seguimiento al cumplimiento de las medidas de seguridad de las bases de datos y repositorios de información que se encuentren en el inventario.

. Identificar y controlar a terceros que realicen tratamiento de datos personales de Protela.

A nivel interno se han establecido procedimientos para la oportuna y eficaz atención de las consultas y reclamos teniendo en cuenta los responsables de las diferentes bases de datos y nuestra estructura administrativa interna. Así pues, a continuación se describe el personal responsable por la custodia y manejo de determinadas bases de datos personales:

**5.3.** Para los datos personales de los trabajadores recolectados de forma física (hojas de vida), reposarán en las oficinas del área de relaciones laborales que cuenta con medidas de seguridad y con acceso limitado a los siguientes trabajadores:

. Director de Talento Humano.
. Director de Gestión de Riesgos y Control Interno.
. Oficial de protección de datos
. Jefe Jurídico.
. Jefe área de Compensación.
. Auxiliares área relaciones laborales.

**5.4.** Para las bases de datos digitales y datos generales de los trabajadores tendrán acceso los cargos anteriores y los siguientes cargos para el desarrollo de su labor y de forma parcial:

. Director de Talento Humano.

. Director de Gestión de Riesgos y Control Interno.
. Oficial de protección de datos.
. Jefe Seguridad y Salud en el Trabajo.
. Jefe Jurídico.
. Jefe de compensación.
. Jefe de Comunicaciones y Bienestar.
. Jefe y Coordinador de Seguridad Física.
. Área de Tecnología para soporte.

**5.5.** Para los datos personales de los clientes recolectados de forma física, reposarán en las oficinas de tesorería que cuenta con medidas de seguridad y con acceso limitado a los siguientes trabajadores:

. Director de Gestión de Riesgos y Control Interno.
. Oficial de protección de datos.
. Jefe Tesorería y Cartera.
. Auxiliares Tesorería y Cartera.
. Coordinador Tesorería y Cartera.
. Asesores Comerciales (para los clientes asignados).
. Área de tecnología para soporte.

**5.6.** Para los datos personales de los proveedores recolectados de forma física, reposarán en las oficinas del área de compras que cuenta con medidas de seguridad y con acceso limitado a los siguientes trabajadores:

. Director de Planeación y Abastecimiento.
. Director de Gestión de Riesgos y Control Interno.
. Oficial de protección de datos.
. Jefe de Compras.
. Auxiliares de Compras.

La siguiente será la tabla de roles y cargos con acceso a las bases de datos de la Compañía:

| **ole** | **Perfiles con manejo directo de datos personales** | **Perfiles con acceso** |
|---|---|---|
| ería y Cartera | Asesor comercial<br>Analista de Tesorería | Ingeniero de tecnología – Oficial de protección de Datos – Director de Gestión |
| mpras y Jefe de comercio exterior | Analista de comercio exterior | Ingeniero de tecnología – Oficial de protección de Datos - Dirección de Riesgo |
| mpensación | Jefe área de relaciones laborales o Jefe Jurídico<br>Personal área relaciones laborales.<br>Personal área de compensación | Ingeniero de tecnología – Oficial de protección de Datos – Director de Riesgos |

## 6. Lineamientos

**6.1. VIGENCIA.**

Protela, aplicará las políticas y procedimientos contenidos en el presente manual a las bases de datos sobre las que tenga poder de decisión, por un término igual al estatutariamente establecido para la duración de la sociedad.

**6.2. PRINCIPIOS.**

Protela guiará todas sus actuaciones relacionadas con el tratamiento de datos personales que realice teniendo en cuenta los siguientes principios:

**. Principio de finalidad:** El tratamiento de datos personales que realiza Protela debe obedecer a una finalidad legítima que se informará al titular.

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

**. Principio de veracidad o calidad:** La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

**. Principio de transparencia:** En el tratamiento debe garantizarse el derecho del titular a obtener de Protela, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

**. Principio de acceso y circulación restringida:** Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados por aquél.

**. Principio de seguridad:** La información sujeta a tratamiento por Protela, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

**. Principio de confidencialidad:** Todas las personas que intervengan en el tratamiento de datos personales están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento.

**. Principio de responsabilidad demostrada:** Es la implementación adecuada de medidas y políticas encaminadas al cumplimiento de la normatividad en materia de protección de datos personales.

**6.3. AUTORIZACIÓN.**

La recolección, almacenamiento, uso, circulación o supresión de datos personales por Protela, requiere del consentimiento libre, previo, expreso e informado del titular de aquellos. Protela, en su condición de responsable del tratamiento de datos personales, ha dispuesto de los mecanismos necesarios para obtener la autorización de los titulares garantizando en todo caso que sea posible verificar el otorgamiento de dicha autorización.

En caso de que Protela actúe como encargado, deberá suscribir los documentos y contratos requeridos por la legislación nacional.

**A. Forma y mecanismos para otorgar la autorización.** La autorización puede darse verbalmente y/o constar en un documento físico, electrónico o cualquier otro formato que permita garantizar su posterior consulta, o mediante un mecanismo técnico o tecnológico idóneo mediante el cual se pueda concluir de forma razonable, que de no haberse surtido una conducta del titular sus datos no hubieren sido almacenados en la base de datos. Con el otorgamiento de la autorización, el titular de los datos personales conoce y acepta que Protela recogerá y utilizará la información para los fines que al efecto le informe de manera previa al otorgamiento de la autorización. En la autorización solicitada por Protela se establecerá:

. Quién y qué datos se recopilan.

. La finalidad del tratamiento de los datos.

. Los derechos de acceso, corrección, actualización o supresión de los datos personales suministrados por el titular.
. Sí se recopilan datos sensibles.

**B. Prueba de la autorización.** Protela adoptará medidas tendientes para mantener registros de cuándo y cómo obtuvo autorización por parte de los titulares de datos personales para el tratamiento de estos.

**C. Casos en que no es necesaria la autorización.** 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 o científicos.

. Datos relacionados con el Registro Civil de las personas.

**D. Suministro de la información.** La información solicitada podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el Titular. La información deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso y deberá corresponder en un todo a aquella que repose en la base de datos.

**E. Deber de informar al titular y aviso de privacidad.** Protela, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente:

. La plena identificación del responsable del tratamiento de los datos personales.

. El tipo de tratamiento al cual serán sometidos los datos y la finalidad del mismo.

. Los mecanismos generales que ha dispuesto Protela para que el titular de la información acceda, conozca y consulte la política de tratamiento de la información adoptada por Protela.

. El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando éstas versen sobre datos sensibles o sobre los datos de niñas, niños y adolescentes.

. Los derechos que le asisten como Titular.

. La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.

Protela conservará el modelo del aviso de privacidad que se transmitió a los titulares mientras se lleve a cabo el tratamiento de datos personales y perduren las obligaciones que de éste deriven. Para el almacenamiento del modelo, Protela podrá emplear medios informáticos, electrónicos o cualquier otra tecnología.

En caso de requerir cámaras o grabaciones de seguridad, estas podrán recoger imágenes o videos para ese único fin y se informará al personal interno y visitante de dicha situación.

**6.4. TITULARES DE LA INFORMACIÓN.**

**A. Derechos de los titulares de la información:** El titular de los datos personales tendrá los siguientes derechos:

. Conocer, actualizar y rectificar sus datos personales frente a Protela 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 a Protela.

. Ser informado por Protela, 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 ley 1581 de 2012 y la presente política, previo agotamiento del procedimiento de reclamaciones establecido por la empresa.

. 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.

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

**Derecho de acceso.** Protela garantizará al titular de la información:

. Acceso a los datos personales que de ese titular posea Protela.

. Información sobre el tratamiento a que son sometidos los datos personales del titular.

. Finalidades que justifican el tratamiento de los datos personales del titular.
Protela garantizará el derecho de acceso cuando, previa acreditación de la identidad del titular se ponga a disposición de éste, de manera gratuita, el detalle de los datos personales a través de medios físicos y/o electrónicos que permitan el acceso directo del titular a ellos. Dicho acceso se ofrecerá por Protela sin límite de plazo y deberá permitir al titular la posibilidad de conocerlos y actualizarlos.

**B. Personas a quienes se les puede suministrar la información.** La información que reúna las condiciones establecidas en la presente ley podrá suministrarse a las siguientes personas:

. A los Titulares, sus causahabientes o sus representantes legales.

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

. A los terceros autorizados por el Titular o por la ley.

**C. Consultas.** Los titulares de la información o sus causahabientes, podrán consultar la información personal del titular que repose en cualquier base de datos de las que sea responsable Protela, quien estará obligado a suministrar a aquellos toda la información contenida en el registro individual o que esté vinculada con la identificación del titular.

Protela garantiza que para atender las solicitudes que le sean hechas con relación a las consultas personales:

. Habilitará los medios de comunicación que considere pertinentes.

. Establecerá mecanismos fáciles y confiables que informará a través del aviso de privacidad.

. Utilizará los canales de atención al cliente que actualmente posee.

Todas las solicitudes de consulta que en este sentido se hagan a Protela, deberán ser atendidas en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de aquella. 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.

**D. Reclamos:** Los titulares de la información o sus causahabientes podrán en cualquier momento y de forma gratuita reclamar a Protela cuando consideren que la información personal de aquellos contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la ley 1581 de 2012 y exigibles a Protela. Dichas reclamaciones se tramitarán así:

. El titular de la información a través del medio predeterminado por Protela elevará el reclamo indicando su identificación, los hechos que dan

lugar a reclamación, informando los datos de contacto y aportando la documentación pertinente que pretenda hacer valer; Sí Protela deduce que el reclamo se presentó de forma incompleta, 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 que Protela reciba un reclamo y no sea competente para resolverlo, dará traslado, en la medida de lo posible, a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

. Cuando la solicitud sea formulada por persona distinta del titular y no se acredite que la misma actúa en representación de aquél, se tendrá por no presentada.

. Una vez Protela reciba un reclamo con el lleno de los requisitos, lo incluirá en sus bases de datos y lo identificará con una leyenda que diga "reclamo en trámite" y el motivo de este, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

. El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo.

Cuando no fuere posible atenderlo dentro de dicho término se informará al interesado antes del vencimiento del referido plazo 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.

. El Titular o causahabiente sólo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante Protela.

En el procedimiento para atender las peticiones, consultas y reclamos, se deberán atender las siguientes instrucciones:

. Protela deberá contar en sus sedes con un área de servicios para la atención de peticiones, consultas y reclamos e implementar mecanismos adicionales, como líneas de atención telefónica o medios virtuales, que garanticen la recepción de las peticiones, consultas y reclamos, de modo ágil y eficaz.

. Las peticiones, consultas y reclamos presentados ante Protela deben ser resueltas de fondo. La respuesta correspondiente debe ser clara, precisa y congruente con lo solicitado.

. Las respuestas a las peticiones, consultas y reclamos presentados ante Protela deben ser comunicadas al Titular de la información, dentro del término establecido en la ley. Tales respuestas deben ser remitidas a la dirección señalada por el Titular en el momento de presentar su solicitud y, en el caso de que no la haya especificado, a la última dirección registrada. En caso de que las peticiones o los reclamos se presenten por medios electrónicos o verbalmente, podrán resolverse por el mismo medio, para lo cual se debe conservar copia de la respuesta o la grabación respectiva.

De acuerdo con lo señalado en el literal b) del numeral 1.5 del Capítulo Primero del Título V de la Circular Única de la Superintendencia de Industria y Comercio, las consultas podrán atenderse por canales electrónicos, siempre y cuando sea posible verificar la identidad del Titular y

garantizar la seguridad de la información.

**E. Rectificación y actualización de datos:** Protela rectificará y actualizará a solicitud del titular, la información de éste que resulte ser incompleta o inexacta, según el procedimiento y los términos señalados en el artículo anterior, siempre y cuando la solicitud de rectificación y/o actualización incluya las correcciones propuestas debidamente fundamentadas.

**F. Supresión de datos:** Los titulares de la información podrán solicitar en cualquier momento a Protela la supresión de sus datos personales.

El titular de la información en todo momento tendrá derecho a solicitar la eliminación total o parcial de sus datos personales a Protela. La supresión de datos operará y será definitiva siempre y cuando los mismos:

. No estén siendo tratados conforme a lo establecido por la legislación vigente.

. Hayan dejado de ser necesarios para la finalidad con la cual se recaudaron.

. Se haya superado el periodo de tiempo requerido para cumplir con el fin con el que se recaudaron.

Protela podrá negar la eliminación cuando:

. El titular tenga el deber legal y/o contractual de permanecer en la base de datos.

. La supresión de los datos obstaculice actuaciones judiciales o administrativas en curso.

. Los datos sean necesarios para proteger los intereses jurídicamente tutelados del titular o para realizar una acción en función del interés público.

**6.5. PROHIBICIONES.**

. Trasladar o sustraer los datos sin autorización.

. Solicitar información diferente a la establecida.

. Hacer uso para su propio beneficio de los datos.

. Cualquier actividad que ponga en riesgo los datos del titular de la información.

. Solicitar el acceso a las bases de datos cuando no cuenta con autorización.

. Suministrar información si no es el titular de los datos personales o no cuenta con la documentación para hacerlo.

**6.6. BASES DE DATOS.**

Protela ha clasificado sus bases de datos de la siguiente manera:

**A. Bases de datos clientes (Confidencial):** Son las bases de datos manuales o automatizadas, que se encuentran estructuradas y que contienen datos de naturaleza pública y privada. La base de datos se encuentra conformada por personas jurídicas y/o naturales.

**B. Bases de datos empleados (Sensible):** Todos los datos suministrados por los empleados, exempleados y pensionados y retirados de Protela. serán tratados, para dar cumplimiento a las obligaciones derivadas de la relación laboral, al ejercicio de los derechos como empleador, al cumplimiento de normatividad o a programas destinados para el personal pensionado o retirado. Toda la información relativa a los empleados o exempleados, serán conservados con el fin de que la Compañía, pueda cumplir sus obligaciones como empleador y ejercer los derechos que en esa misma condición le corresponden, de acuerdo con la legislación laboral colombiana. Al momento del ingreso a Protela los nuevos empleados deberán conocer, aceptar y aplicar las Políticas de Protección de Datos Personales. Para dar por finalizado el proceso de vinculación de un nuevo empleado en Protela, es necesario garantizar que el empleado firme y acepte el programa integral de gestión de datos.

Respecto al Tratamiento de Datos Sensibles, estos se prohíben, excepto cuando:

. El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.

. El Tratamiento sea necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.

. El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular.

. El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

. El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

**C. Bases de datos de proveedores y contratistas (Confidencial):** Protela tramitará los datos comerciales e información financiera que considere necesaria para el cumplimiento de su objeto social y para la celebración de contratos con terceros. Los datos de los mismos, serán tratados con la intimidad, derechos a la privacidad, el buen nombre de las personas, dentro del proceso del tratamiento de datos personales, y durante todas las actividades se respetarán los principios de confidencialidad, seguridad, legalidad, acceso, libertad y transparencia. Para tal efecto, se reglamenta la firma del Acuerdo de Confidencialidad para la entrega de Datos con todos los proveedores.

**6.7. RECOLECCIÓN DE DATOS PERSONALES.**

**A. Almacenamiento físico datos de los Titulares de la información:**

**. Clientes:** Los datos de los clientes se recolectan al momento de ser inscritos en el sistema corporativo y esta función se encuentra a cargo del asesor comercial con revisión por parte del área de Tesorería y Cartera. La constancia de la recolección reposará en la carpeta de los clientes nacionales y en la carpeta de los clientes internacionales según corresponda.

**. Trabajadores:** Los datos suministrados por los trabajadores de Protela se recolectan una vez realizada su vinculación a la compañía, los cuales deberán manifestar su conformidad con la autorización de tratamiento de datos personales, esta función de recolección de datos está a cargo de las áreas de Compensación y Nómina. Las hojas de vida de los empleados se encuentran en físico en el archivo de las anteriores áreas.

**. Proveedores:** Los datos suministrados por el proveedor se recolectan una vez se crea el perfil en el sistema corporativo manifestando así su aceptación de la autorización de tratamiento de datos, esta función se encuentra a cargo del área de compras y la autorización reposará en dicha área.

B. Almacenamiento digital y control de seguridad. El Almacenamiento digital de los datos personales se realizará en el software Queryx para trabajadores, SAP, Apoteosys y NOW para proveedores y SAP, Apoteosys, NOW y AngelNet para clientes, esto para los datos que reposen en bases de datos electrónicas o digitales.

**C. Finalidades de la recolección de datos:**

**1. Clientes:**

. Desarrollar actividades comerciales y de mercadeo. Incluidas campañas telefónicas, mailing, estudio de mercado y cualquier otro tipo de actividad relacionada con mercadeo, por cualquier medio conocido o por conocer. Para tal fin podrá compartir los datos con aliados comerciales o proveedores con el fin de desarrollar la actividad o campaña.

. Transferir los Datos Personales a las Entidades Vinculadas, con el fin de ser tratados para las finalidades descritas en esta autorización.
. Gestionar el cumplimiento de obligaciones legales, precontractuales, contractuales o poscontractuales

. Verificar la identidad del titular, realizar estudios de seguridad y/o aplicar los protocolos de seguridad a fin de prevenir y mitigar el riesgo de fraude, lavado de activos y/o financiación del terrorismo, entre otras.

. Cumplimiento de obligaciones contractuales, por lo cual la información podrá ser transferida a terceros, tales como entidades financieras, notarías, abogados, etc.

. Para dar cumplimiento a las obligaciones contraídas con clientes y proveedores, atención al cliente, acreditación, consolidación actualización, tramitación, fortalecer las relaciones con clientes y proveedores mediante el envió de información relevante.

**2. Trabajadores:**

. Control de ingreso y egreso de la Compañía.

. Participación en procesos de selección.

. Identificación plena de la persona.

. Gestión administrativa.

. Estadística e informes internos.

. Verificación en listas restrictivas y/o antecedentes judiciales cuando se requiera y la ley lo permita.

. Realizar el tratamiento de datos sensibles de condiciones específicas de salud con el fin de realizar la prevención de riesgos laborales.

. Investigación epidemiológica y actividades análogas.

. Realizar el tratamiento de datos sensibles como huellas dactilares o un cálculo sobre ellas, fotografías, imágenes de video, ubicación espacial, datos de ordenadores, teléfonos y números celulares, VPN, correo electrónico, que serán utilizados con fines de autenticación e identificación por medio de la firma electrónica y/o digital con el fin de verificar la autenticidad de la autorización. Dicha información será almacenada y utilizada adicionalmente para ofrecer una capa adicional de seguridad. Conozco que no estoy obligado a autorizar el tratamiento de los datos sensibles a menos que sea estrictamente necesario para alguno de los fines descritos o requeridos por ley.

. Suministrar, transmitir, transferir información personal, laboral y financiera para que sea conocida y tratada por las personas naturales o jurídicas, filiales, matrices, accionistas, vinculados económicos o aliados comerciales de Protela como entidades bancarias, entidades de formación, aliados, proveedores nacionales o extranjeros, que presten servicios tecnológicos, logísticos, operativos, estadísticos y/o de cualquier otro tipo.

. Realizar actuaciones en caso de emergencia.

. Evaluaciones de desempeño.

. Control de ingreso de equipos de cómputo y/o software o de elementos de valor.

. Capacitación y/o entrenamiento sobre los procesos de Protela, sus productos y/o servicios.

. Exámenes periódicos.

. Actividades e investigaciones relacionadas con Seguridad y Salud en el Trabajo.

. Encuestas para cumplimiento de obligaciones legales y/o consolidación de estadísticas.

. Divulgación de campañas comerciales de Protela y/o sus sociedades vinculadas.

. Invitaciones para actividades de bienestar y/o remisión de obsequios.

. Visitas domiciliarias.

. Contestación de requerimientos de entidades estatales.

. Divulgación de Campañas de comunicación interna o externa. Para lo cual podrá utilizar datos sensibles como fotografías, siluetas, videos, audios e ilustraciones personales, lo cual se autoriza expresamente con el presente documento.

. Divulgación de imágenes, fotografías, videos, audios para campañas de marca empleadora de uso externo e interno.

**3. Proveedores:**

. Control de ingreso y egreso de la Compañía.

. Proveer servicios y productos requeridos.

. Informar a sus colaboradores, clientes, proveedores y terceros sobre cumplimiento y cambios en los productos y servicios contratados y/o por contratar.

. Realizar estudios internos sobre el cumplimiento de las relaciones comerciales y estudios de mercado a todo nivel.

. Responder requerimientos legales de entidades administrativas y judiciales.

. Identificación plena de la persona y cumplimiento de legislación.

. Gestión administrativa.

. Estadística e informes internos.

. Verificación en listas restrictivas y/o antecedentes judiciales cuando se requiera y la ley lo permita.

. Realizar el tratamiento de datos sensibles como Huellas dactilares o un cálculo sobre ellas, fotografías, imágenes de video, ubicación espacial, datos de ordenadores, teléfonos y números celulares, VPN, correo electrónico, que serán utilizados con fines de autenticación e identificación por medio de la firma electrónica y/o digital con el fin de verificar la autenticidad de la autorización. Dicha información será almacenada y utilizada adicionalmente para ofrecer una capa adicional de seguridad. Conozco que no estoy obligado a autorizar el tratamiento de los datos sensibles a menos que sea estrictamente necesario para alguno de los fines descritos o requeridos por ley.

. Suministrar, transmitir, transferir información personal y financiera para que sea conocida y tratada por las personas naturales o jurídicas, filiales, matrices, accionistas, vinculados económicos o aliados comerciales de Protela como entidades bancarias, entidades de formación, aliados, proveedores nacionales o extranjeros, que presten servicios tecnológicos, logísticos, operativos, estadísticos y/o de cualquier otro tipo.

. Cumplimiento de obligaciones financieras frente al proveedor.

. Realizar actuaciones en caso de emergencia.

. Control de ingreso de equipos de cómputo y/o software o de elementos de valor.

. Capacitación y/o entrenamiento sobre los procesos de Protela, sus productos y/o servicios.

. Encuestas para cumplimiento de obligaciones legales y/o consolidación de estadísticas.

. Revisión de propuestas comerciales e invitación a ofertar.

. Contestación de requerimientos de entidades estatales.

Al llegar a existir cambios en las finalidades de los tratamientos de datos personales de alguna de las bases de datos administradas por la compañía, se informará a los titulares mediante correo electrónico registrado directamente en la base datos.

**D. Uso de los datos personales:** El uso de los datos personales se encuentra limitado al autorizado por el titular en el documento establecido por Protela o en cualquier anexo que se llegara a presentar.

**E. Eliminación o disposición final:** La eliminación de los datos personales de las bases de datos de Protela se realizará de acuerdo con la solicitud del titular de la información siempre y cuando no haya una obligación legal de mantener los datos personales por un periodo de tiempo determinado. Si el titular de los datos no realiza ninguna solicitud de eliminación, se dispondrá:

. Permanencia indefinida para los empleados en virtud de dar cumplimiento de normatividad legal.

. Eliminación de estos datos después de 10 años de inactividad para datos de clientes y/o proveedores.

**6.8. MEDIDAS DE SEGURIDAD.**

Protela adoptará las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; Dichas medidas responderán a los requerimientos mínimos hechos por la legislación vigente y periódicamente se evaluará su efectividad.

Protela aplicará políticas de seguridad de la información que permitan proteger, preservar y administrar los atributos de confidencialidad, integridad, disponibilidad y autenticidad de la información.

**A. Transferencia de datos internacionales:** Protela no realiza transferencia de datos personales internacionales, pero en caso de requerirlo cumplirá con la normatividad vigente sobre el tema y suscribirá los contratos o cláusulas de transferencia de datos internacionales. Así pues, en caso de que se llegase a presentar, se prohíbe la transferencia de datos personales de cualquier tipo 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 cumple 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 ley 1581 de

2012 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.

**B. Implementación de las medidas de seguridad:** Protela mantendrá protocolos de seguridad de obligatorio cumplimiento para el personal con el acceso a los datos tratados.

**6.9. PROCEDIMIENTO DE SEGURIDAD.**

El procedimiento se describe a continuación:

**A. Ámbito de aplicación del procedimiento:** Bases de datos y documentación relacionada sobre trabajadores, proveedores y clientes.

**B. Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad:** Protela tiene como propósito principal proteger la información frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad, disponibilidad y confiabilidad de la información.

**C. Funciones y obligaciones del personal a cargo del tratamiento de datos:**

. Velar por la implementación efectiva de las políticas y procedimientos adoptados por ésta, para cumplir la norma de protección de datos personales.

. No delegar las funciones relacionadas con datos personales.

**D. Estructura de las bases de datos de carácter personal y descripción de los sistemas de información que los tratan:** El acceso a las bases de datos se encuentra debidamente administrado con mecanismos de control de acceso, autenticación, validación y auditoría.

**E. Procedimiento de notificación, gestión y respuesta ante las incidencias:** Si se llegare a identificar alguna falla en la seguridad del tratamiento de datos como adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento por parte de cualquier persona con acceso o no a las bases de datos, esta deberá ser informada al oficial de protección de datos personales, y él será el encargado de verificar la severidad de estos hechos junto con el área tecnológica.

La severidad del incidente puede ser:

**. Alto impacto:** El incidente de seguridad afecta a activos de información considerados de impacto catastrófico y mayor que influyen directamente a los objetivos misionales de Protela. Se incluyen en esta categoría aquellos incidentes que afecten la reputación y el buen nombre o involucren aspectos legales. Estos incidentes deben tener respuesta inmediata por parte del oficial de datos, deberá realizar un requerimiento especifico al área encargada, una vez obtenida la respuesta, el oficial de datos personales verificara si existió o no incidencia de seguridad debiendo informar a la junta directiva y haciendo el reporte especifico ante la Superintendencia de Industria y Comercio entre los siguientes 15 días hábiles. Si es el caso, realizar la denuncia penal ante la autoridad competente

**. Medio impacto:** El incidente de seguridad afecta a activos de información considerados de impacto moderado que influyen directamente a los objetivos de un proceso determinado, pero sin llegar a afectar las bases de datos personales, en este caso no se realizará reporte de incidencia ante la Superintendencia de Industria y Comercio.

**. Bajo impacto:** El incidente de seguridad afecta a activos de información considerados de impacto menor e insignificante, que no influyen en ningún objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto y no se reportarán ante la Superintendencia de Industria y Comercio.

**F. Procedimiento interno de incidencias:** Estará a cargo del oficial de datos personales y el jefe del Área en donde haya ocurrido la Incidencia, debiendo realizar por lo menos el siguiente procedimiento:

. Identificar Causas.

. Evaluar medidas disciplinarias de acuerdo con el Reglamento Interno de Trabajo.

. Evaluar la eficacia de los procesos para evitar su recurrencia.

**G. Procedimientos de realización de copias de respaldo y de recuperación de los datos:** El área de tecnología de la Compañía cuenta con procedimientos de realización de copias de respaldo y su periodicidad está contemplada de acuerdo con la información manejada por cada cargo.

**H. Controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el procedimiento de seguridad que se implemente:** El área de competitividad y auditoría deberán controlar dichos procesos.

**I. Medidas a adoptar cuando un soporte o documento vaya a ser transportado, desechado o reutilizado:**

. Copia digital de respaldo cuando se realice por fuera de la empresa.

. Acompañamiento de personal que tenga funciones de tratamiento de datos personales cuando se realice de forma interna.

. Reporte ante la Superintendencia de Industria y Comercio en caso de desechar base de datos completa y acta de destrucción total por parte del área encargada y del oficial de tratamiento de datos personales.

**J. Procedimiento de actualización de bases de datos:** Se actualizará de acuerdo con la normatividad que se expida sobre habeas data o con los hallazgos que se hayan realizado por parte del oficial de datos.

**K. Auditorías internas:** Se realizarán periódicamente verificando el cumplimiento de procedimientos y efectividad de los controles, enmarcados en la política de seguridad informática.

**6.10. GESTIÓN DEL RIESGO.**

**A. Matriz de riesgos:** Los siguientes funcionarios deberán tener dentro de su gestión de riesgos la inclusión del tratamiento de habeas data:

. Gerente de tecnologías de la información.

. Jefe área jurídica.

. Jefe área de compensación.

. Asesores de negocios.

**B. Nuevos negocios:** El oficial de datos, una vez reciba la comunicación por parte del área comercial o directiva de la compañía, de un nuevo negocio o área donde deba incursionar Protela revisará de forma detallada si se están solicitando nuevos datos personales.

Se incluirá en todos los medios contractuales de la empresa la cláusula de confidencialidad.

**6.11. ENTRENAMIENTO Y CAPACITACIÓN.**

**A. Inducción de ingreso a trabajadores:** La inducción responde a la necesidad de integrar al nuevo trabajador a la cultura organizacional de Protela, los objetivos principales son:

. Iniciar su integración al sistema deseado por la entidad, así como el fortalecimiento de su formación ética e importancia de los datos personales.

. Familiarizarlo con las funciones generales, la organización, la empresa y los datos personales.

. Instruirlo acerca de la misión de la entidad y de las funciones de su dependencia, al igual que sus responsabilidades individuales, sus deberes y derechos, y prohibiciones respecto a los datos personales.

Esta inducción se puede llevar a la práctica a través de metodologías presenciales o virtuales, la inducción personal se puede hacer de manera

presencial en el recinto donde el nuevo empleado va a desarrollar sus funciones, esta inducción estará a cargo del área de Relaciones Laborales o Capacitación, que cuenta con personal capacitado para abarcar los diferentes temas de esta.

**B. Inducción a empleados con acceso a bases de datos:** El proceso de inducción a los nuevos empleados se llevará a cabo con la explicación y capacitación de recolección, almacenamiento y tratamiento de datos personales suministrados por empleados, clientes y proveedores. Este proceso consiste en realizar una familiarización con el acceso a bases de datos para que su manejo sea adecuado por parte de ellos teniendo en cuanta la normatividad vigente y las regulaciones establecidas por Protela.

**C. Reinducción Corporativa a trabajadores:** La reinducción tiene como objetivo principal reorientar al empleado en virtud de los cambios producidos en cualquiera de los asuntos a los cuales se refieran sus objetivos. La reinducción se debe impartir una vez al año si se presentan cambios que afecten directamente las obligaciones o funciones del empleado o sobre la normatividad. Para los trabajadores con acceso a las bases de datos esta deberá tener en cuenta la actualización legal acerca del tratamiento de datos personales o cualquier modificación interna ejercida por Protela.

Los registros de dichas capacitaciones serán controlados y archivados por parte del área de selección y formación de la Compañía.

**6.12. CANAL DE COMUNICACIÓN**

Para el reporte de cualquier novedad relacionada con la presente política, Protela habilitó los siguientes canales de comunicación directos con la compañía:

**- Oficial.cumplimiento@protela.com**
**- Tel. (601) 2916600 Ext. 1248**

## 7. Régimen Sancionatorio

La Dirección de Talento Humano de Protela definió de acuerdo con la legislación laboral y el Reglamento Interno de Trabajo, el régimen disciplinario general que se aplicará cuando exista incumplimiento de esta Norma.

En caso de incumplimiento por parte de alguno de los accionistas, Directivos y empleados a la Política Integral de Gestión de Datos Personales, la Compañía pondrá en marcha sus procedimientos disciplinarios y sancionatorios establecidos en los contratos de trabajo, en sus Políticas de Cumplimiento y/o en el Reglamento Interno de Trabajo, así como en las normas laborales aplicables para el efecto.

Este mecanismo sancionatorio se activará en caso de que alguno de los empleados, accionistas, y/o Directivos de Protela:

. Realicen alguna conducta contraria a la presente Política; y toleren y/o consientan dichas conductas.

. Estén enterados de alguna conducta contraria a la presente Política; y toleren y/o consientan dichas conductas; y/o no la informen en tiempo.

. No cumplan con sus funciones de acuerdo con el Programa y las demás Políticas de Cumplimiento.

**7.1. SANCIONES LABORALES.**

En el artículo 49 del RIT se mencionan las faltas leves y sus respectivas sanciones disciplinarias, así pues, se establece que:

"El error u omisión en el ingreso de información en la base de datos del empleador, que traiga como consecuencia la falta de cobro de los servicios prestados a terceros, la pérdida de información, o perjuicios económicos al empleador, implica por primera vez suspensión del contrato de trabajo hasta por tres (3) días" .

Por otra parte, el artículo 50 del RIT establece las faltas graves las cuales podrán dar lugar hasta la terminación del contrato por justa causa, y en su numeral 3 menciona como una de estas faltas graves la siguiente:

"3. Violación directa a la cláusula de confidencialidad, Habeas Data, Sagrilaft, PTEE y Derechos Humanos estipulada en el contrato de trabajo" (Subrayado por fuera del texto original).

El numeral 13 del artículo 50 establece que:

"13. El error u omisión por segunda vez en el ingreso de información en la base de datos del empleador, que traiga como consecuencia la falta de cobro de los servicios prestados a terceros, la pérdida de información, o perjuicios económicos al empleador".

El numeral 15 del artículo 50 establece que:

"15. Acceder de forma remota o presencial a la base de datos, o al servidor (s) de información del empleador, o de la empresa a la cual se le preste servicios, para extraer información en beneficio propio, o de un tercero".

Así mismo, en el numeral 44 del anterior artículo se establece como falta grave que dará lugar hasta la terminación del contrato por justa causa lo siguiente:

"44. Cuando al trabajador se le compruebe cualquier actividad que vaya en contravención de los postulados y obligaciones contemplados en las políticas de Prevención de Actividades Referidas al Lavado de Activos, Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva, Política de Transparencia y Ética Empresarial, Política de Derechos Humanos y Política Integral de Gestión de Datos Personales" (Subrayado por fuera del texto original).

En ese orden de ideas, se ejecutará el procedimiento establecido en el CAPÍTULO XVII "PROCEDIMIENTOS PARA COMPROBACIÓN DE FALTAS Y FORMAS DE APLICACIÓN DE LAS SANCIONES DISCIPLINARIAS" para proveer el debido proceso a favor del empleado y sobre la comprobación real de las faltas imputadas.

**7.2. SANCIONES PENALES.**

Según lo consagrado en el Artículo 269F del Código Penal, la sanción que se establece para las personas que cometan el delito de "Violación de datos personales" es la siguiente:

"El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes".

Además de las sanción anteriormente descrita, se aplicarán todas las demás sanciones de carácter penal permitidas por el Código Penal Colombiano y la normatividad penal vigente según corresponda. En el caso de que dichas conductas se presenten en territorio extranjero en razón a la ejecución de labores de la empresa como por ejemplo la realización de negocios comerciales, se tendrá en cuenta el principio de territorialidad de la ley, el cual se entiende como la posibilidad de que un Estado aplique las normas de su ordenamiento dentro del territorio bajo su dominio, sin interferencia alguna de otros Estados.

**7.3. SANCIONES ADMINISTRATIVAS.**

. Multas de carácter personal e institucional hasta por dos mil (2.000) salarios mínimos mensuales legales vigentes.

. Suspensión de las actividades relacionadas con el tratamiento hasta por seis (6) meses.

. Cierre temporal de las operaciones relacionadas con el tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la SIC.

. Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles.

En cuanto a los criterios para graduar las anteriores sanciones administrativas, la ley 1581 de 2012 en su artículo 24 estableció que dichas sanciones se graduarán atendiendo los siguientes criterios, en cuanto resulten aplicables:

. La dimensión del daño o peligro a los intereses jurídicos tutelados por la ley en mención.

. El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción.

. La reincidencia en la comisión de la infracción.

. La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio.

. La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio.

. El reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.

En consecuencia, el colaborador que por su acción u omisión dolosa o gravemente culposa conlleve a que la empresa sea sancionada administrativamente, será sujeto a la aplicación de la sanción laboral a que haya lugar en base al procedimiento establecido en el CAPÍTULO XVII "PROCEDIMIENTOS PARA COMPROBACIÓN DE FALTAS Y FORMAS DE APLICACIÓN DE LAS SANCIONES DISCIPLINARIAS" del

Reglamento Interno de Trabajo de Protela.

Los representantes de la compañía, directivos, asociados, colaboradores y en especial el oficial de cumplimiento, declaran conocer las disposiciones y sanciones administrativas y penales por incumplimiento a las instrucciones impartidas por la Superintendencia de Industria y Comercio en materia de gestión de datos personales, de acuerdo con lo previsto en la Ley Estatutaria 1581 de 2012 "por el cual se dictan disposiciones generales para la protección de datos personales".

## 8. Cumplimiento Normativo

El presidente, los directores, los gerentes y los jefes son los principales responsables por la divulgación, seguimiento y control de lo establecido en esta Política. La Auditoría Interna vigilará el cumplimiento en sus ciclos de auditoría y pondrá en conocimiento de la Junta Directiva, Presidencia y/o Gerencia respectiva los hallazgos que evidencie.

## 9. Anexos

| VERSIÓN | FECHA | RAZÓN DE LA ACTUALIZACIÓN |
|---|---|---|
| 2 | 05/OCT/2023 | Actualización de documento |

| ELABORÓ | | REVISÓ | | APROBÓ | |
|---|---|---|---|---|---|
| **Nombre:** | JEIMY GERALDIN MONSALVE CHURQUE | **Nombre:** | MARIA ALEJANDRA TOVAR PAEZ | **Nombre:** | MARIA ALEJANDRA TOVAR PAEZ |
| **Cargo:** | AUXILIAR DE GESTION DOCUMENTAL | **Cargo:** | DIRECTOR DE TALENTO HUMANO | **Cargo:** | DIRECTOR DE TALENTO HUMANO |
| **Fecha:** | 05/Oct/2023 | **Fecha:** | 05/Oct/2023 | **Fecha:** | 05/Oct/2023 |