Política para el Tratamiento de la Información Personal - Colombia

Prosegur Ciberseguridad SAS.

Contenido

1. INTRODUCCIÓN

Prosegur Ciberseguridad SAS. garantiza la protección de los derechos de Hábeas Data, privacidad, intimidad, buen nombre, e imagen, y con tal propósito todas sus actuaciones se regirán siempre por principios de buena fe, legalidad, autodeterminación informática, libertad y transparencia.

La sociedad **Prosegur Ciberseguridad SAS.** domiciliada en la ciudad de Bogotá en la **cra 19 No. 68 B - 76,** con dirección electrónica www.prosegur.com.co, con teléfonos (+601) 3444420 y correo electrónico habeasdata.colombia@prosegur.com (quién en adelante se denominará como "la empresa"), en cumplimiento de su objeto social y en ejercicio de sus actividades ocasionales o permanentes actúa como Responsable o como Encargado del tratamiento de datos personales. Así mismo, dada la pertenencia de **Prosegur Ciberseguridad SAS.** al Grupo Empresarial **PROSEGUR**, es común que parte de la información personal administrada por la empresa, particularmente la que refiere a reportes, resultados e información estadística o asociada a servicios de servidores de información, sea compartida con la casa matriz del Grupo, o con empresas filiales o pertenecientes al Grupo Empresarial y aliados comerciales con acuerdo vigente, quienes actuarán como Encargadas del tratamiento de **Prosegur Ciberseguridad SAS.** y excepcionalmente también podrán actuar como Responsables de tratamiento. Por esta razón y para dar cumplimiento a la ley de protección de datos, se expide la presente Política de Tratamiento de la Información Personal, la cual busca dar a conocer los principios y directrices que guían el tratamiento de datos personales por la empresa, logrando de esta forma fortalecer la confianza de los titulares de la información personal cuando aquellos entreguen sus datos personales a Prosegur Ciberseguridad SAS., para su tratamiento.

2. MARCO NORMATIVO

1. El Artículo 15º de la Constitución Política de Colombia establece el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, tanto de entidades públicas como privadas. Así mismo, este derecho comprende otras facultades como las de autorizar el tratamiento, incluir nuevos datos, excluirlos o suprimirlos de una base de datos o archivo.[1]

2. En el año 2008 se expidió la Ley Especial de Hábeas Data[2], que regula lo que se ha denominado como el "habeas data financiero", es decir el derecho que tiene todo individuo a conocer, actualizar y rectificar su información personal, comercial, crediticia y financiera contenida en centrales de información públicas o privadas, que tienen como función recopilar, tratar y circular esos datos con el fin de determinar el nivel de riesgo financiero de su titular. Esta ley considera titular de la información tanto a las personas naturales como las jurídicas.

3. En octubre de 2012 se expidió la Ley 1581, "Ley General de Protección de Datos Personales", que desarrolla el derecho de Habeas Data desde una perspectiva más amplia que la financiera y crediticia. Así, cualquier titular de datos personales tiene la facultad de controlar la información que se ha recolectado de sí mismo en cualquier base de datos o archivo, sea administrado por entidades privadas o públicas.

   Bajo esta Ley General es titular del dato la persona natural. Solamente, en ocasiones especiales podría serlo una persona jurídica.[3]

[1] De acuerdo con la sentencia C-748 de 2011 de la Corte Constitucional

[2] Ley 1266 de 2008, Ley Especial de Hábeas Data.

[3] Situaciones especiales previstas por la Corte Constitucional, Sentencia C-748 de 2011

De acuerdo con lo anterior, en el Decreto 1377 de 2013 Artículo 27, dispone que las Organizaciones establezcan Políticas Internas efectivas para garantizar:

1. Una estructura administrativa en la Organización, proporcional a su estructura, para implementar las Políticas Adoptadas.
2. Mecanismos internos para poner en práctica las políticas, incluyendo herramientas de implementación, entrenamiento y programas de educación.
3. La adopción de procesos para la atención de reclamos y consultas de los Titulares.

3. ÁMBITO DE APLICACIÓN

La presente Política será aplicable a todos los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento directamente por **Prosegur Ciberseguridad SAS**. como Responsable, así como también será aplicable por los terceros que obren en nombre de **Prosegur Ciberseguridad SAS.** como sus Encargados.

Así mismo, la presente Política será aplicable a todos los datos personales a los que, con ocasión a la tipología de los servicios prestados, **Prosegur Ciberseguridad SAS**. acceda y trate por cuenta del Responsable del tratamiento y, consecuentemente, actúe como Encargado del tratamiento. Lo dispuesto en esta Política se complementará con las obligaciones establecidas en los contratos de prestación de servicios y acuerdos de tratamiento de datos que **Prosegur Ciberseguridad SAS**. firme en calidad de prestador de servicios y Encargado.

4. OBJETIVOS

I. **Prosegur Ciberseguridad SAS.** y las empresas que conforman el Grupo Empresarial **PROSEGUR** están firmemente comprometidas con la Protección de los Datos de carácter personal que trata en el transcurso de su actividad, con el objetivo principal de proteger los derechos y libertades fundamentales de las personas físicas, y en particular, su derecho a la protección de los datos personales.

II. Con el fin de llevar a cabo este compromiso y de dar cumplimiento a las obligaciones en materia de Protección de Datos, según lo previsto en la Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”, del Decreto 1377 de 2013 y demás normas aplicables, hemos desarrollado la presente Política para el Tratamiento de la Información Personal que tiene por objetivo formalizar los principios que todo empleado de **Prosegur Ciberseguridad SAS.** y las empresas que conforman el Grupo Empresarial **PROSEGUR** debe conocer y cumplir en materia de protección de datos.

5. DEFINICIONES

De conformidad con la legislación vigente, se determinan las siguientes definiciones para la interpretación de la presente política:

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

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

3. **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

4. Dato personal sensible: Datos personales que por su carácter pueden afectar la intimidad del titular o cuyo uso indebido puede generar su discriminación.

5. 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.

6. Habeas Data: Derecho fundamental contenido en el artículo 15 de la Constitución Política, el cual garantiza a toda persona el derecho a conocer, actualizar y rectificar la información personal que se haya recogido sobre ella en archivos y bancos de datos de naturaleza pública o privada.

7. 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 personales.

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

9. Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

10. 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.

11. Transmisión de Datos: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia, con el objeto de que un Encargado realice tratamiento por cuenta del Responsable.

6. PRINCIPIOS DE CUMPLIMIENTO EN MATERIA DE PROTECCIÓN DE DATOS

Prosegur Ciberseguridad SAS. aplicará los siguientes principios, los cuales constituyen las reglas a seguir en la recolección, manejo, uso, tratamiento, almacenamiento e intercambio de datos personales:

1. **Principio de finalidad:** El tratamiento debe obedecer a una finalidad legítima, de acuerdo con la Constitución y la Ley, y debe ser informada al titular.

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

3. **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.

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

5. **Principio de acceso y circulación restringido:** El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales y de las disposiciones de la presente ley y la Constitución. En este sentido, el tratamiento sólo puede estar a cargo de personas autorizadas por el titular y/o por las personas previstas en esta ley. Los datos personales, salvo la información pública, no pueden estar disponibles en internet ni en otros medios de

divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la Ley General.

6. **Principio de seguridad:** La información sujeta a tratamiento por parte del responsable del tratamiento o del Encargado del tratamiento se debe manejar con las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

7. **Principio de confidencialidad:** Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando corresponda al desarrollo de las actividades autorizadas en la Ley General y en los términos de ésta.

8. **Principio de necesidad y proporcionalidad:** Los datos personales registrados en una base de datos deben ser los estrictamente necesarios para el cumplimiento de la finalidad del tratamiento, la cual debe ser comunicada al titular. En consecuencia, los datos que se solicitan deben ser adecuados, pertinentes y acordes con esa finalidad del Tratamiento.

9. **Principio de temporalidad o caducidad:** El periodo de conservación de los datos personales será aquel necesario para alcanzar la finalidad para la cual se han recolectado.

10. **Principio de legalidad en materia de tratamiento de datos:** El tratamiento a que se refiere esta Ley es una actividad regulada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.

7. DEBERES DE PROSEGUR CIBERSEGURIDAD SAS. EN EL TRATAMIENTO DE DATOS PERSONALES

7.1. Cuando Prosegur Ciberseguridad SAS. actúe como Responsable del tratamiento de datos personales

a. Garantizar al titular en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
b. Solicitar y conservar, en las condiciones previstas en la ley, copia de la respectiva autorización otorgada por el titular.
c. Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
d. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
e. Garantizar que la información que se suministre al Encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
f. Actualizar la información, comunicando de forma oportuna al Encargado del tratamiento, todas las novedades respecto de los datos personales que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.
g. Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del tratamiento.
h. Suministrar al Encargado del tratamiento, según el caso, únicamente datos personales cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la ley.
i. Exigir al Encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular.

j. Tramitar las consultas y reclamos formulados en los términos señalados en la ley.
k. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y en especial, para la atención de consultas y reclamos.
l. Informar al Encargado del tratamiento cuando determinada información se encuentra en discusión por parte del titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
m. Informar a solicitud del titular sobre el uso dado a sus datos personales.
n. Informar a la autoridad de protección de datos personales cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información personal de los titulares.
o. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

7.2. Cuando Prosegur Ciberseguridad SAS. actúe como Encargado del tratamiento de datos personales:

a. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
b. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
c. Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la ley.
d. Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.
e. Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la ley.
f. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares.
g. Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la presente ley.
h. Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
i. Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
j. Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
k. 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.
l. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

8. TRATAMIENTO DE DATOS PERSONALES POR PROSEGUR CIBERSEGURIDAD SAS.

8.1. Recolección de autorizaciones

Sin perjuicio de las excepciones previstas en la ley, para el tratamiento de datos personales se requiere de la autorización previa, expresa e informada del titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta y verificación posterior.

Prosegur Ciberseguridad SAS. recolectará las respectivas autorizaciones, las cuales pueden constar tanto en un documento físico o electrónico, o en cualquier otro formato que permita garantizar su posterior consulta, así como mediante un mecanismo técnico o tecnológico

idóneo, que permita manifestar u obtener el consentimiento vía grabación telefónica o click durante la navegación de páginas web o formularios en línea.

En el mismo sentido, se entenderá que la autorización cumple con estos requisitos cuando se manifieste (i) por escrito, (ii) de forma oral o (iii) las autorizaciones también podrán obtenerse mediante una conducta inequívoca del titular, de la cual se pueda concluir de manera razonable, que el titular otorgó autorización, y que, de no haberse surtido aquella conducta del titular, los datos nunca hubieren sido capturados y almacenados en la base de datos.

Para dar cumplimiento a lo anterior, se podrán establecer archivos físicos o repositorios electrónicos realizados de manera directa por la empresa o a través de terceros contratados para tal fin.

En los casos en los cuales **Prosegur Ciberseguridad SAS**. actúe como Encargado, el Responsable de los datos será quien debe asegurar y conservar la autorización previa, expresa e informada de la autorización del tratamiento de los datos personales, emitida por el titular de los mismos.

8.2. Tratamiento de información que no requiere autorización del titular

No se recolectará la autorización del titular para el tratamiento sus datos, cuando el tratamiento de los mismos esté inmerso en alguno de las siguientes excepciones:

a. Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
b. Datos de naturaleza pública.
c. Casos de urgencia médica o sanitaria.
d. Tratamiento de información autorizado por la ley para fines históricos, estadístico o científicos.
e. Datos relacionados con el registro civil de las personas.

8.3. Tratamiento y finalidades a las que serán sometidos los datos personales

Los datos personales son siempre de propiedad de las personas a las que se refieren y sólo aquellas pueden decidir sobre los mismos. En este sentido, **Prosegur Ciberseguridad SAS**. hace uso de los datos sólo para aquellas finalidades para las que se encuentra debidamente facultado por la ley o autorizado por el titular, y en todo caso respetando la normatividad vigente sobre protección de datos personales.

En todo caso, y para aquellos datos que no sean de naturaleza pública, los mismos solo serán revelados con la expresa autorización del titular o cuando una autoridad competente lo solicite.

Particularmente las finalidades para las que son empleados los datos al interior de **Prosegur Ciberseguridad SAS.** son:

8.4. Tratamiento de datos personales en calidad de Responsable

8.4.1. Trabajadores

La información de los trabajadores será tratada **manual** y **automáticamente** con la **finalidad** de administrar la relación laboral entre **Prosegur Ciberseguridad SAS.** y el trabajador o colaborador, y particularmente para:

1. Cumplir las obligaciones a cargo del empleador, determinadas por la ley laboral colombiana o que hayan sido impartidas por autoridades competentes.

2. Gestionar el pago de la nómina y la seguridad social, lo que puede incluir realizar registros en portales bancarios.

3. Entregar dotación al trabajador.

4. Ejecutar y evidenciar la participación del trabajador en entrenamientos, actividades, talleres, capacitaciones y plan de formación.

5. Adelantar procedimientos disciplinarios.

6. Implementar el denominado Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST).

7. Crear y administrar los usuarios que permiten el acceso a las plataformas (software) de la empresa y de correos electrónicos.

8. Mantener comunicación a través de e-mail, teléfono, mensajes de texto (SMS y/o MMS), mensajería instantánea o de cualquier otro medio de comunicación;

9. Realizar entrevista con polígrafo, para cumplir con los requisitos de los clientes (en los casos que se requiera);

10. Evaluar el desempeño, las habilidades y competencias en el desarrollo de las funciones diarias;

11. Realizar las actividades programadas por bienestar para mejorar el clima laboral;

12. Realizar los registros contables que obliga la ley;

13. Consultar y/o verificar su información en listas de control Nacional e Internacional relacionadas con Lavados de Activos y Financiación del Terrorismo;

14. Adelantar procesos de calificación de origen y porcentaje de pérdida de capacidad laboral en los cuales sea parte el trabajador(a);

15. Presentar solicitudes y trámites pensionales;

16. Contactar a familiares en casos de emergencia;

17. Emitir certificados laborales y brindar referencias laborales a quien las solicite;

18. Datos personales sensibles como la imagen, captada por cámaras de seguridad, serán tratados con la finalidad de controlar el ingreso a las instalaciones de la empresa, velar por la seguridad, y promover ambientes de trabajo sanos.

19. Datos personales sensibles como la imagen, captada en fotografías, serán tratados con la finalidad de realizar la documentación del personal con carné, conservar soporte de las actividades recreativas o culturales y de bienestar, registro de la temperatura al ingresar a las instalaciones, así como realizar publicaciones internas o externas, como en la página web o redes sociales de la empresa y las actividades inherentes a las labores del cargo.

20. Datos personales sensibles como la voz e imagen captada en teleconferencias, celular corporativo o reuniones virtuales, serán tratados con la finalidad registrar la realización de eventos en general y las actividades inherentes a las labores del cargo.

21. Datos personales sensibles como la voz captada en llamadas de call center , serán tratados con la finalidad de llevar un registro de la calidad de las funciones prestadas por los trabajadores, y permitir su consulta posterior.

22. Datos personales sensibles como la huella, serán tratados con la finalidad de acreditar el consentimiento en asuntos contractuales.

23. Datos de carácter sensible como el seguimiento a síntomas de salud, serán recolectados con la única finalidad de cumplir los protocolos de bioseguridad por emergencias sanitarias y por pandemias.

24. Realizar comunicaciones de carácter comercial acerca de la empresa o del grupo empresarial al que pertenece.

25. Realizar perfilados y actividades de analítica predictiva con objeto de estudiar y predecir comportamientos y mejorar la productividad de la empresa.

26. Realizar proyectos de automatización de procesos de negocio para mejorar los productos y servicios ofrecidos por la empresa.

27. Circulación de la información por Transmisión y/o transferencia de acuerdo con lo descrito en el numeral 8.4.1 de la presente Política.

28. Las demás contenidas en la respectiva autorización o aviso de privacidad.

La información recolectada de trabajadores corresponderá principalmente a datos de identificación, datos de ubicación, datos relacionados con la historia laboral y experiencia profesional del trabajador, e información socioeconómica. Para el caso de los trabajadores, la información personal que soporte el SG-SST será conservada por el término de veinte (20) años a partir de la finalización de la relación laboral de acuerdo a lo ordenado por la Resolución 312 de 2019, y la información de la historia laboral relacionada con contribuciones a parafiscales y seguridad social en general, será almacenada por el termino de ochenta (80) años a partir de la finalización de la relación laboral de acuerdo a las circunstancias legales o contractuales que hagan necesario la conservación de la información.

8.4.2. Familiares y beneficiarios de los trabajadores

La información de los familiares y beneficiarios de los trabajadores será tratada manual y automáticamente con la finalidad de cumplir las obligaciones laborales a cargo **de Prosegur Ciberseguridad SAS.** y particularmente para:

1. Cumplir las obligaciones a cargo del empleador, determinadas por la ley laboral colombiana o que hayan sido impartidas por autoridades competentes.

2. Realizar y gestionar la realización de afiliaciones de los beneficiarios de los trabajadores a la seguridad social y cajas de compensación.

3. Realizar y conservar soporte de las actividades de bienestar, recreativas o culturales y del desarrollo de las diferentes actividades propias de una relación laboral.

4. Realizar notificaciones de algún caso de emergencia en el que el colaborador de Prosegur se vea involucrado.

La información recolectada de familiares y beneficiarios de los trabajadores corresponderá principalmente a datos de identificación. Dicha información será conservada por el mismo término que sea conservada la información personal del trabajador por quien sus datos son tratados por la empresa, considerando además las circunstancias legales o contractuales que pudieran hacer necesario el tratamiento por un término adicional.

8.4.3. Trabajadores retirados

La información de los extrabajadores se trata manual y automáticamente con la finalidad de suministrar información general a los interesados sobre la relación laboral que existió entre la **Prosegur Ciberseguridad SAS.** y el trabajador o colaborador, y particularmente para:

1. Emitir certificados laborales, y brindar referencias laborales a quien las solicite.

2. Atender solicitudes de consulta por parte de sus titulares, causahabientes o aquellos que la ley autorice a realizar consultas.

3. Cumplir con las obligaciones que impone la ley laboral colombiana.

La información recolectada de los extrabajadores corresponderá principalmente a datos de identificación, datos de ubicación, datos relacionados con la historia laboral y experiencia profesional del trabajador, e información socioeconómica. Para el caso de los ex trabajadores, la información personal que soporte el SG-SST será conservada por el término de veinte (20) años a partir de la finalización de la relación laboral de acuerdo a lo ordenado por la Resolución 312 de 2019, y la información de la historia laboral relacionada con contribuciones a parafiscales y seguridad social en general, será almacenada por el termino de ochenta (80) años a partir de la finalización de la relación laboral de acuerdo a las circunstancias legales o contractuales que hagan necesario la conservación de la información.

8.4.4. Candidatos, aspirantes o participantes en procesos de selección

La información de los candidatos será tratada manual y automáticamente con la finalidad de seleccionar personal para la empresa y finalmente concretar una relación laboral entre el aspirante y **Prosegur Ciberseguridad SAS.** y particularmente para:

1. Permitir el desarrollo de los procesos de selección de la empresa.

2. Verificar la veracidad de la información aportada y rectificar las referencias personales y/o laborales proporcionadas.

3. Consultar antecedentes disciplinarios y/o judiciales.

4. Realizar pruebas psicotécnicas, psicofísicas, y/o entrevista con polígrafo, así como exámenes médicos de ingreso.

5. Realizar estudios de seguridad, lo que puede incluir la realización de visitas domiciliarias.

6. Datos personales sensibles como la huella, serán tratados con la finalidad de acreditar el consentimiento en asuntos contractuales.

7. Consultar y/o verificar su información en listas de control Nacional e Internacional relacionadas con Lavados de Activos y Financiación del Terrorismo.

8. Formalizar la relación contractual, lo que comprenderá el proceso de contratación.

9. Enviar comunicaciones relacionadas con futuras posiciones o procesos de selección para vacantes de la empresa o del Grupo Empresarial al que pertenece.

La información recolectada de candidatos corresponderá principalmente a datos de identificación, datos de ubicación, datos relacionados con la historia laboral y experiencia profesional del trabajador. Para el caso de los candidatos, la información personal será conservada por el término de seis (6) meses, contado a partir del momento que el aspirante haya finalizado su participación en el proceso de selección al cual aplicó, considerando además las circunstancias legales o contractuales que pudieran hacer necesario el tratamiento por un término adicional.

8.4.5. Clientes

La información de los clientes personas naturales y Representantes Legales de los clientes personas jurídicas será tratada manual y automáticamente con la finalidad de administrar la relación entre **Prosegur Ciberseguridad SAS.** y el cliente, y particularmente para:

1. Permitir la perfección de la relación comercial que lo vincula con **Prosegur Ciberseguridad SAS.**

2. Realizar actividades comerciales con aliados, lo que puede implicar verificación y consulta, de información financiera, crediticia o comercial con los operadores de bancos de datos o centrales de riesgo, para verificar el riesgo crediticio o de reporte histórico de comportamiento comercial.

3. Permitir la ejecución del objeto comercial contratado, y cumplimiento de las obligaciones contraídas por **Prosegur Ciberseguridad SAS.**

4. Gestionar las etapas precontractual, contractual y pos contractual, lo que puede incluir la realización de actividades de cobro adelantadas directamente por la empresa organización o a través de un tercero que la realice a nombre de la empresa o a su propio nombre.

5. Realizar reportes o actualizaciones de información financiera, crediticia o comercial a los operadores de bancos de datos o centrales de riesgo.

6. Atender posventas y solicitudes de garantía.

7. Realizar evaluación de calidad a los servicios, así como estudios para estadísticas y análisis de tendencias del mercado.

8. Realizar invitaciones a eventos programados por la empresa.

9. Consultar y/o verificar su información en listas de control Nacional e Internacional relacionadas con Lavados de Activos y Financiación del Terrorismo.

10. Realizar actividades de fidelización de clientes y operaciones de marketing.

11. Realizar actos de promoción y publicidad de los servicios de **Prosegur Ciberseguridad SAS.**, así como de los terceros que formen parte del Grupo Empresarial y de aliados comerciales con acuerdo vigente, para la prestación de servicios complementarios o conexos a los ofrecidos por Prosegur Vigilancia y Seguridad Privada.

12. Datos personales sensibles como la huella, serán tratados con la finalidad de acreditar el consentimiento en asuntos contractuales y debidas diligencias relacionadas con Lavado de Activos y Financiación del Terrorismo.

13. Datos personales sensibles como la voz captada por la grabación de llamadas y de call center, serán tratados con la finalidad de evaluar la calidad del servicio, la consecución de la autorización de tratamiento de los datos recolectados durante la llamada. y permitir su posterior consulta

14. Datos personales sensibles como la voz e imagen captada en teleconferencias o reuniones virtuales, serán tratados con la finalidad registrar la realización de eventos en general.

15. Mantener comunicación a través de e-mail, teléfono, mensajes de texto (SMS y/o MMS), mensajería instantánea o de cualquier otro medio de comunicación, que permita mantener una eficiente comunicación.

16. Envío de ofertas comerciales, concertación de visitas, realización de acciones de fidelización, atención de reclamaciones

17. Contacto con los funcionarios del cliente previamente autorizados, dentro del árbol de decisión de reporte de situaciones de peligro o emergencia en los servicios de ciberseguridad.

18. Realizar los registros contables que obliga la ley.

19. Enviar la información a entidades gubernamentales, públicas o privadas por solicitud expresa de las mismas o por exigencia legal.

20. Circulación de la información por Transmisión y/o transferencia de acuerdo con lo descrito en el numeral 8.4.1 de la presente Política.

21. Realizar proyectos de automatización de procesos de negocio para mejorar los productos y servicios ofrecidos por la empresa.

22. Cumplir las obligaciones a cargo de la empresa, determinadas por la ley o que hayan sido impartidas por autoridades competentes.

23. Las demás contenidas en la respectiva autorización o aviso de privacidad.

La información recolectada de clientes corresponderá principalmente a datos de identificación, datos de ubicación relacionados con la actividad comercial del cliente, información socioeconómica por solicitarse copia del RUT y datos relacionados con sus intereses para permitir la prestación de los servicios ofertados por la empresa organización.

Dicha información personal será conservada por el tiempo que se encuentre vigente la relación comercial o contractual entre **Prosegur Ciberseguridad SAS.** y el cliente, y cinco (5) años más, atendiendo al interés que manifieste la persona en los productos o servicios ofertados por Prosegur Ciberseguridad SAS. independiente de las circunstancias legales o contractuales que pudieren hacer necesario un tratamiento por un término adicional.

8.4.6. Potenciales Clientes

La información de los potenciales clientes será tratada manual y automáticamente con la finalidad de promover la consolidación de una relación comercial entre el potencial cliente y **Prosegur Ciberseguridad SAS**., y particularmente para:

1. Compartir el portafolio de productos y/o servicios de la empresa.

2. Presentar ofertas de servicios y permitir el desarrollo de la etapa de negociación precontractual, para consolidar la relación comercial entre el potencial cliente y la empresa.

3. Realizar estudios de crédito, lo que puede implicar verificación y consulta, de información financiera, crediticia o comercial con los operadores de bancos de datos o centrales de riesgo, para verificar el riesgo crediticio o de reporte histórico de comportamiento comercial.

4. Atender las inquietudes o preguntas que sean presentadas por el potencial cliente. Mantener una eficiente comunicación, a través de e-mail, teléfono, mensajes de texto (SMS y/o MMS), mensajería instantánea o de cualquier otro medio de comunicación, que permita mantener una eficiente comunicación con los potenciales clientes.

5. Realizar actos de promoción y publicidad de los servicios de **Prosegur Ciberseguridad SAS.** así como de los terceros que sean empresas pertenecientes al Grupo Empresarial y de aliados comerciales con acuerdo vigente, para la prestación de servicios complementarios o conexos a los ofrecidos por **Prosegur Ciberseguridad SAS.**

6. Realizar invitaciones a eventos programados por la empresa.

7. Adelantar actividades de marketing y/o publicidad.

8. Datos personales sensibles como la voz e imagen captada en teleconferencias o reuniones virtuales, serán tratados con la finalidad registrar la realización de eventos en general y permitir su posterior consulta y difusión interna o externa al público en medios de comunicación.

9. Circulación de la información por Transmisión y/o transferencia de acuerdo con lo descrito en el numeral 8.4.1 de la presente Política.

10. Las demás contenidas en la respectiva autorización o aviso de privacidad.

La información recolectada de potenciales clientes corresponderá principalmente a datos de identificación, datos de ubicación, y datos relacionados con sus intereses para permitir el desarrollo de actividades de publicidad y marketing. Dicha información personal será conservada por el tiempo de un (1) año más, contado a partir del momento que el potencial cliente haya realizado su última manifestación de interés en los servicios ofertados por **Prosegur Ciberseguridad SAS.**, considerando además las circunstancias legales o contractuales que pudieren hacer necesario el tratamiento por un término adicional.

8.4.7. Proveedores o contratistas

La información de los proveedores o contratistas será tratada manual y automáticamente con la finalidad de administrar la relación contractual entre **Prosegur Ciberseguridad SAS.** y el proveedor o contratista, y particularmente para:

1. Verificar la idoneidad y competencia del Proveedor o Contratista, y/o sus trabajadores.

2. Desarrollar el proceso de evaluación y selección de proveedores.

3. Verificar antecedentes disciplinarios, fiscales y/o penales, así como la inclusión del proveedor en listas de riesgos o listas restrictivas.

4. Consultar y/o verificar su información en listas de control Nacional e Internacional relacionadas con Lavados de Activos y Financiación del Terrorismo.

5. Formalizar y cumplir con la documentación requerida dentro de los procesos de inscripción y registro de Proveedores o Contratistas.

6. Permitir la perfección de la relación comercial que lo vincula con **Prosegur Ciberseguridad SAS.**, lo que puede implicar el trato de datos de carácter sensible en la suscripción o reconocimiento de documentos en los que se proporcione huella.

7. Permitir la ejecución del objeto comercial contratado, y cumplimiento de las obligaciones contraídas por **Prosegur Ciberseguridad SAS.**

8. Gestionar los pagos a que haya lugar por la prestación de servicios o suministro de bienes, lo que puede incluir realizar registros en portales bancarios.

9. Emitir certificados, y brindar referencias a quien las solicite.

10. Requerir en caso de aclaraciones, garantías o auditorias.

11. Evaluar la calidad de los servicios teniendo en cuenta los niveles de servicio recibidos de los proveedores.

12. Mantener una eficiente comunicación de la información que sea de utilidad en los vínculos contractuales entre la empresa y sus Proveedores y Contratistas.

13. Datos personales sensibles como la huella, serán tratados con la finalidad de acreditar el consentimiento en asuntos contractuales.

14. Datos personales sensibles como la voz e imagen captada en teleconferencias o reuniones virtuales, serán tratados con la finalidad registrar la realización de eventos en general y permitir su posterior consulta y difusión interna o externa al público en medios de comunicación.

15. Realizar los registros contables que obliga la ley.

16. Enviar la información a entidades gubernamentales, públicas o privadas por solicitud expresa de las mismas o por exigencia legal.

17. Cumplir las obligaciones a cargo de la empresa, determinadas por la ley o que hayan sido impartidas por autoridades competentes.

18. Realizar comunicaciones de carácter comercial acerca de la empresa o del grupo empresarial al que pertenece.

19. Las demás contenidas en la respectiva autorización o aviso de privacidad.

La información recolectada de proveedores y contratistas corresponderá principalmente a datos de identificación y datos de ubicación relacionados con el desempeño de una profesión o de un oficio para permitir la prestación del servicio o adquisición de productos por parte de **Prosegur Ciberseguridad SAS.** Dicha información personal será conservada por el tiempo que se mantenga vigente la relación comercial o contractual entre **Prosegur Ciberseguridad SAS.** y el proveedor o contratista más cinco (5) años, y el adicional que las circunstancias legales o contractuales exijan.

8.4.8. Representantes legales y personas de contacto de clientes, proveedores o contratistas

La información de los representantes legales y personas de contacto de clientes, proveedores o contratistas que estén constituidos como personas jurídicas, será tratada manual y automáticamente con la finalidad de administrar la relación contractual entre **Prosegur Ciberseguridad SAS.** y el cliente, proveedor o contratista, y particularmente para:

1. Permitir la perfección de la relación comercial que lo vincula con **Prosegur Ciberseguridad SAS.**, lo que puede implicar el trato de datos de carácter sensible en la suscripción o reconocimiento de documentos en los que se proporcione imagen o huella.

2. Formalizar la inscripción y registro en la empresa como cliente, proveedor o contratista.

3. Permitir la ejecución del objeto comercial contratado y cumplimiento de las obligaciones contraídas por **Prosegur Ciberseguridad SAS.**

4. Realizar evaluación de calidad a los servicios, así como estudios para estadísticas y análisis de tendencias del mercado.

5. Mantener una eficiente comunicación, a través de e-mail, teléfono, mensajes de texto (SMS y/o MMS), mensajería instantánea o de cualquier otro medio de comunicación.

6. Datos personales sensibles como la huella, serán tratados con la finalidad de acreditar el consentimiento en asuntos contractuales y debidas diligencias relacionadas con Lavado de Activos y Financiación del Terrorismo.

7. Datos personales sensibles como la imagen y huella digital captada en la cédula de ciudadanía o en formularios, serán tratados para formalizar el registro como proveedor y conservar prueba de la firma en los formularios que suscriba.

8. Realizar los registros contables que obliga la ley.

9. Consultar y/o verificar su información en listas de control Nacional e Internacional relacionadas con Lavados de Activos y Financiación del Terrorismo.

10. Cumplir las obligaciones a cargo de la empresa, determinadas por la ley o que hayan sido impartidas por autoridades competentes.

11. Realizar comunicaciones de carácter comercial acerca de la empresa o del grupo empresarial al que pertenece.

12. Circulación de la información por Transmisión y/o transferencia de acuerdo con lo descrito en el numeral 8.4.1 de la presente Política.

13. Las demás contenidas en la respectiva autorización o aviso de privacidad.

La información recolectada de representantes legales y personas de contacto de clientes, proveedores o contratistas que estén constituidos como personas jurídicas corresponderá principalmente a datos de identificación y datos de ubicación relacionados con el desempeño de una profesión o de un oficio para la persona jurídica que obra como cliente, proveedor o contratista de **Prosegur Ciberseguridad SAS.** Dicha información personal será conservada por el tiempo **Prosegur Ciberseguridad SAS.** y el cliente, y cinco (5) años más, atendiendo al interés que manifieste la persona en los servicios ofertados por Prosegur Ciberseguridad SAS.,

independiente de las circunstancias legales o contractuales que pudieren hacer necesario un tratamiento por un término adicional.

8.4.9. Accionistas

La información de los accionistas personas naturales y/o beneficiarios finales de los accionistas personas jurídicas será tratada manual y automáticamente con la finalidad de administrar la relación entre **Prosegur Ciberseguridad SAS.** y los socios, y particularmente para:

1. Invitar a reuniones de la sociedad, y en general ejercer los deberes y derechos de todo socio;
2. Emitir certificaciones de la calidad de socio.
3. Realizar el registro en los libros societarios de la empresa.
4. Permitir el pago de dividendos en caso de repartición de utilidades.
5. Realizar los registros contables que obliga la ley.
6. Realizar inscripciones ante el registro mercantillas y/o autoridades correspondientes que sean necesarias en cumplimiento de la ley como el envío de información de beneficiarios finales ante la Dian.
7. Datos personales sensibles como la huella, serán tratados con la finalidad de acreditar el consentimiento en asuntos contractuales y debidas diligencias relacionadas con Lavado de Activos y Financiación del Terrorismo.
8. Consultar y/o verificar su información en listas de control Nacional e Internacional relacionadas con Lavados de Activos y Financiación del Terrorismo.
9. Contactar para envío de comunicaciones y notificaciones relativas al desarrollo de la empresa. Realizar comunicaciones de carácter comercial acerca de la empresa o del grupo empresarial al que pertenece.
10. Las demás contenidas en la respectiva autorización o aviso de privacidad.

La información recolectada de accionistas corresponderá principalmente a datos de identificación, datos de ubicación y datos de carácter socioeconómico. De un lado, la información personal reportada en el libro de accionistas será conservada por el mismo tiempo que la sociedad se encuentre vigente, y por el otro, la información de identificación y de contacto tratada por el área administrativa, será almacenada por el tiempo que la persona conserve su calidad de accionista y cinco (5) años más, independiente de las circunstancias legales o contractuales que pudieren hacer necesario un tratamiento por un término adicional.

8.4.10. Visitantes de las instalaciones físicas de la empresa

La información de los visitantes será tratada manual y automáticamente con la finalidad de realizar los controles de administración para el ingreso y salida a las instalaciones físicas de la empresa, y particularmente para:

1. La imagen captada por las cámaras de seguridad se conservará por la empresa de manera temporal para promover la seguridad de los espacios vigilados.

2. Permitir el ingreso únicamente a personas que cuentan con la autorización de ingreso por parte de la persona a quién visitan.

3. Llevar registro de las visitas realizadas.

4. Identificar a las personas que se encuentren en las instalaciones de la empresa y usar sus datos en caso de una emergencia o siniestro según lo ordena el SG-SST.

5. Compartir con terceros en caso de que una autoridad competente por realización de investigaciones policivas o motivos de seguridad lo requiera.

6. Las demás contenidas en la respectiva autorización o aviso de privacidad.

La información recolectada de visitantes corresponderá principalmente a datos de identificación, datos relacionados con la profesión o el oficio, datos de ubicación y de contacto. Dicha información personal será conservada por treinta (30) días contados a partir de su recolección, y el adicional que las circunstancias legales o contractuales hagan necesario.

8.4.11. Tratamiento de los datos de niños, niñas y adolescentes

De acuerdo con el Artículo 7 de la Ley 1581 de 2012 y al objeto social de **Prosegur Ciberseguridad SAS**., la empresa no recolecta ni realiza tratamiento de datos personales de menores de edad como parte de su actividad comercial. Sin embargo, en el marco de las relaciones de carácter laboral para cumplir con las obligaciones a cargo del empleador, y para permitir el desarrollo de las actividades programadas para el bienestar de los trabajadores y sus familias, la empresa recolectará datos de hijos y beneficiarios de trabajadores que sean menores de edad.

Cuando **Prosegur Ciberseguridad SAS.** realice el tratamiento de datos personales de menores de edad, la empresa garantiza el respeto a los derechos prevalentes de los menores, se asegura de solicitar las respectivas autorizaciones a los representantes o tutores de los menores, y adopta medidas de seguridad suficientes para asegurar la confidencialidad, integridad, disponibilidad, reserva y circulación restringida de dichos datos personales.

8.4.12. Tratamiento de datos personales de carácter sensible

Para el tratamiento de datos sensibles, **Prosegur Ciberseguridad SAS.** informará al Titular de los datos lo siguiente:

1. Para el tratamiento de este tipo de información el Titular no está obligado a dar su autorización o consentimiento.
2. Se informará de forma explícita y previa qué tipo de datos sensibles serán solicitados.
3. Se comunicará el tratamiento y la finalidad que se le dará a los datos sensibles.
4. La autorización de los datos sensibles será previa, expresa y clara.

En el marco de las relaciones de carácter laboral para cumplir con las obligaciones a cargo del empleador, para acreditar el consentimiento en asuntos contractuales, y para permitir la ejecución de los procesos de seguridad que controlan las instalaciones de la empresa organización, se recolectarán datos personales de carácter sensible relacionados con el estado de salud de los trabajadores, y datos biométricos de trabajadores y visitantes que puedan quedar registrados en los videos de seguridad.

8.5. Tratamiento de datos personales en calidad de Encargado

En los casos en los cuales dentro del alcance del servicio contratado por el cliente, **Prosegur Ciberseguridad SAS.** actúe como Encargado del tratamiento, los datos se tratarán en base a la relación contractual entre el cliente y Prosegur con, entre otras, las siguientes finalidades:

1. Prestar servicios de Servicios de Seguridad Gestionada Managed Security Services (MSS), Monitorización de Ciberseguridad e inteligencia de Ciberseguridad dentro de la condiciones del servicio contratado y durante la vigencia del contrato.
2. Trasmitir internacionalmente y de manera temporal los datos en los servidores mantenidos por Prosegur.
3. Controlar el acceso de empleados, proveedores y visitantes a las instalaciones del cliente
4. Gestión de incidencias y reclamaciones por parte del cliente.

8.6. Transferencia y Transmisión Nacional e Internacional de Datos Personales

8.6.1. Transferencia y Transmisión Nacional

La información personal de **trabajadores, proveedores, accionistas, clientes, potenciales clientes** o **potenciales proveedores** tratada por **Prosegur Ciberseguridad SAS.** en calidad de Responsable del tratamiento y, en su caso, como Encargado del Tratamiento, podrá circular en transmisión o en transferencia con terceros externos a la empresa ubicados en el territorio nacional, en los siguientes casos:

a. Con autoridades gubernamentales o públicas, incluidas, entre otras autoridades judiciales o administrativas, autoridades fiscales, organismos de control y/o de investigación penal, civil, administrativa, disciplinaria y/o fiscal.

b. Con profesionales, asesores y proveedores necesarios en procedimientos legales, judiciales, contables, financieros, administrativos, tecnológicos, de auditoría, de innovación y de asesoría empresarial en general de cuya función sea necesaria para: i) Cumplir con las leyes vigentes, ii) Responder a las solicitudes de las autoridades y del gobierno, iii) Diseñar y/o actualizar procedimientos internos a la empresa. iv) Atender procesos judiciales, v) Recibir asesoría profesional o especializada, entre otros.

c. Con cualquiera de las empresas que conforman el Grupo Empresarial **PROSEGUR** al que pertenece **Prosegur Ciberseguridad SAS**. y cuya circulación sea necesaria para la ejecución de proceso administrativo u operativos y permitir el seguimiento y desarrollo de los procesos corporativos.

d. Con cualquiera de las empresas que sean aliados que cuenten con acuerdos comerciales asociados, para los fines del desarrollo de las funciones de la prestación de los servicios propios y de aquellos mencionados en el alcance de los acuerdos comerciales asociados con **Prosegur Ciberseguridad SAS.**

Prosegur Ciberseguridad SAS. tomará las medidas necesarias para que los terceros Encargados de la empresa conozcan y se comprometan a observar la presente Política, bajo el entendido de que la información personal transmitida, únicamente podrá ser utilizada para asuntos directamente relacionados con el objeto social de **Prosegur Ciberseguridad SAS.** y con la finalidad con la que fueron recolectados, y no podrá ser usada o destinada para propósito o fin diferente.

8.6.2. Transferencia y Transmisión Internacional

La información personal de trabajadores, proveedores, accionistas y clientes de **Prosegur Ciberseguridad SAS**., es transmitida internacionalmente con ocasión de la delegación en terceros del servicio de almacenamiento de la información en servidores externos a la compañía, los cuales se encuentran ubicados fuera del país. En dichos casos, **Prosegur Ciberseguridad SAS.** se asegura que el país al que sean transmitidos los datos proporcione niveles adecuados de protección de datos, los cuales en ningún caso podrán ser inferiores a los fijados en Colombia por la Ley Estatutaria 1581 de 2012; y tomará las medidas necesarias para que los terceros que obren como Encargados, solo puedan usar la información proporcionada con la finalidad con la que fue recolectados, y no pueda ser usada o destinada para propósito o fin diferente. Así mismo, en la transmisión internacional de datos la empresa suscribirá un acuerdo de transmisión en los términos del artículo 25 del Decreto 1377 de 2013, o en su defecto le informará de la transmisión a los respectivos titulares para obtener su consentimiento.

Así mismo, la información personal de trabajadores, proveedores, accionistas y clientes de **Prosegur Ciberseguridad SAS.** es transferida internacionalmente con ocasión de la pertenencia de la empresa a un grupo empresarial de carácter internacional. En dichos casos, **Prosegur Ciberseguridad SAS.** se asegura que, el país al que sean transferidos los datos proporcione niveles adecuados de protección de datos, el titular haya otorgado su autorización para la transferencia y adopta las medidas apropiadas y efectivas para garantizar la seguridad y el adecuado tratamiento de los datos personales transferidos.

9. DERECHOS DE LOS TITULARES

Atendiendo a lo dispuesto en la normatividad vigente y aplicable en materia de hábeas data o protección de datos personales, el titular tiene los siguientes derechos:

a. Conocer, rectificar y actualizar sus datos personales frente a **Prosegur Ciberseguridad SAS.**, en su condición de Responsable del tratamiento.

b. Solicitar prueba de la autorización otorgada a **Prosegur Ciberseguridad SAS.**, en su condición de Responsable del tratamiento.

c. A recibir información por parte de **Prosegur Ciberseguridad SAS**., previa solicitud, respecto del uso que dado a sus datos personales.

d. Acudir ante las autoridades legalmente constituidas, en especial ante la Superintendencia de Industria y Comercio, y presentar quejas por infracciones a lo dispuesto en la normatividad vigente en las normas aplicables, previo trámite de consulta o requerimiento ante el Responsable del tratamiento.

e. Modificar y revocar la autorización y/o solicitar la supresión sus datos personales cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales vigentes.

f. Tener conocimiento y acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

10. EJERCICIO DE LOS DERECHOS POR PARTE DE LOS TITULARES

Prosegur Ciberseguridad SAS. cuenta con una organización administrativa que le permite atender las solicitudes, consultas y reclamos en general que se presenten en torno al tratamiento de datos personales realizado al interior de la empresa. Para lo anterior, se informa

el área encargada de llevar a cabo la función de protección de datos personales, y por lo tanto, quien dará trámite a las solicitudes de los Titulares, para el ejercicio de sus derechos; así como también se informa el canal de atención, para que sea usado por los titulares para la presentación de Consultas y Reclamos:
Área designada:

La Dirección Legal y de Cumplimiento desempeña la función de protección de datos, y por lo tanto, es el área que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos.

Canal de atención:

El correo electrónico habeasdata.colombia@prosegur.com

10.1. Consultas

Los titulares, así como los causahabientes, representantes y/o apoderados de titulares, debidamente acreditados, podrán consultar la información personal del titular que repose en cualquier base de datos de **Prosegur Ciberseguridad SAS. En consecuencia, Prosegur Ciberseguridad SAS.** garantizará el derecho de consulta y acceso, suministrando a los titulares, toda la información contenida en el registro individual del titular o que esté vinculada con su identificación.

Las Consultas serán atendidas en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recibo. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado antes del vencimiento de los diez (10) días mencionados, 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 plazo.

10.2. Reclamos

Los titulares, así como los causahabientes, representantes y/o apoderados del titular debidamente acreditados, que consideren que la información contenida en una base de datos debe ser objeto de corrección, rectificación, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la ley, podrán presentar un Reclamo ante **Prosegur Ciberseguridad SAS.,** remitiéndolo a través del área designada para ejercer la función de protección de datos personales al interior de la empresa.

Un Reclamo se podrá presentar de forma gratuita, previa acreditación de la identidad del titular, causahabiente, representante o apoderado.

Los Reclamos serán atendidas en un término máximo de quince (15) días hábiles contados a partir del día siguiente de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado antes del vencimiento de los quince (15) días mencionados, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer plazo.

Todo reclamo deberá contener como mínimo la siguiente información, siguiendo lo indicado en el artículo 15 de la Ley 1581 de 2012:

a. La identificación del titular.
b. Los documentos que acrediten la identidad o la personalidad del titular, causahabiente, representante o apoderado.

c. La descripción de los hechos que dan lugar al reclamo, con la descripción clara y precisa de los datos personales respecto de los cuales el titular busca ejercer alguno de los derechos.
d. La dirección de notificación o cualquier otro medio para recibir la respuesta.
e. Los documentos que se quiera hacer valer.

En caso de presentarse un Reclamo incompleto, en el término de cinco (5) días hábiles siguientes a su recepción, se solicitará la información faltante al interesado para que subsane. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del Reclamo.

10.3. Supresión de datos

Los titulares tienen el derecho, en todo momento, a solicitar la supresión de sus datos personales. Esta supresión implica la eliminación total o parcial de la información personal de acuerdo con lo solicitado por el titular.
La supresión de los datos personales no es un derecho absoluto **y Prosegur Ciberseguridad SAS.** como Responsable del tratamiento puede negar su ejercicio cuando:

a. El titular tenga un deber legal o contractual de permanecer en la base de datos.
b. La eliminación de los datos represente un obstáculo para el ejercicio de actuaciones judiciales o administrativas.

10.4. Revocatoria de la autorización

Los titulares de los datos personales pueden revocar el consentimiento al tratamiento de sus datos personales en cualquier momento, siempre y cuando no lo impida una disposición legal o contractual.

La revocación del consentimiento puede darse dos modalidades; la primera, puede ser sobre la totalidad de las finalidades consentidas, esto es,que **Prosegur Ciberseguridad SAS.** deba dejar de tratar por completo los datos del titular; la segunda, es la revocación parcial del consentimiento, la cual puede ocurrir sobre finalidades determinadas, como por ejemplo para fines publicitarios o de estudios de mercado, manteniendo a salvo otros fines del tratamiento de conformidad con la autorización otorgada por el titular.

10.5. Requisito de procedibilidad

La presentación de quejas para el ejercicio de sus derechos ante la Superintendencia de Industria y Comercio solo será procedente una vez el interesado haya agotado el trámite de Consulta o Reclamo directamente **Prosegur Ciberseguridad SAS.** como Responsable.

10.6. Actualización de información personal

La actualización de datos de las contrapartes (clientes, proveedores, trabajadores) se realizará acorde a los tiempos estipulados por cada área y o negocio de acuerdo con los lineamientos que se tengan para actualizar los datos de sus contrapartes involucradas.

11. AVISO DE PRIVACIDAD

El aviso de privacidad es el documento físico, electrónico o en cualquier otro formato conocido o por conocer, que es puesto a disposición del titular por parte de **Prosegur Ciberseguridad SAS.** para el tratamiento de sus datos personales. A través de este documento se informa 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.

Prosegur Ciberseguridad SAS. empleará avisos de privacidad para atender el derecho de los titulares a ser informados, los cuales serán dispuestos en las comunicaciones electrónicas, y en lugares visibles durante la realización de todo evento o reunión en la cual se recolecten datos personales para informar a los titulares acerca del tratamiento.

12. USO DEL MATERIAL AUDIOVISUAL (VIDEO VIGILANCIA) DE NUESTRAS INSTALACIONES

Las instalaciones **Prosegur Ciberseguridad SAS.** y del Grupo Empresarial **Prosegur** cuentan con un sistema de seguridad de video vigilancia que tiene como finalidad garantizar la seguridad de los bienes, instalaciones y personas que se encuentran en las instalaciones como elemento de persuasión y de disuasión. Las cámaras de video vigilancia estarán instaladas de forma fija en zonas comunes y visibles que no violen la intimidad de las personas que están siendo monitoreadas.

Con el fin de informar a los Titulares de los datos personales que se encuentran dentro de una zona de Video vigilancia, se han instalado Avisos visibles en los que además se informan los derechos que le asisten a los Titulares de los Datos y la manera como estos pueden ser ejercidos.

Las situaciones por las cuales se puede consultar las grabaciones de las cámaras de video vigilancia son:

- Hurto y/o daño de cualquier elemento de la oficina.
- Conducta irregular de funcionarios, proveedores, visitantes y/o terceros.
- Acceso a lugares no autorizados.
- En caso de emergencia (incendio, temblor, catástrofes y/o fenómenos naturales).
- Incumplimiento a protocolos de bioseguridad dentro de las instalaciones de Prosegur.

Las personas que tienen acceso a las grabaciones son los colaboradores autorizados los cuales tienen la función de monitorear el buen funcionamiento de estas y gestionar el material audiovisual cuando sea requerido.
La solicitud de la copia de la grabación se debe realizar a través de los canales establecidos por la Gerencia de Riesgos.

12.1. Vigencia y Modificación de esta Política

La presente Política es objeto de las adecuadas acciones en comunicación, formación y sensibilización para su oportuna comprensión y aplicación en **Prosegur Ciberseguridad SAS.**

La presente política rige a partir del 13 de septiembre de 2022 y deja sin efectos los reglamentos o manuales especiales que se hubiesen expedido con anterioridad. En todo caso, **Prosegur Ciberseguridad SAS.** se reserva el derecho de modificar la misma en cualquier momento, comunicando a los interesados oportunamente su entrada en vigencia.

© 2022 Prosegur Ciberseguridad SAS. Todos los derechos reservados.