



MANUAL DE POLÍTICA DE PRIVACIDAD Y TRATAMIENTO DE DATOS PERSONALES

FUNDACIÓN SILARAA

AGOSTO DE 2024

V. 01



TABLA DE CONTENIDO

1. JUSTIFICACIÓN.....	3
2. OBJETIVO.....	4
3. ALCANCE.....	5
4. PRINCIPIOS.....	5
5. DEFINICIONES.....	6
6. ROLES EN MATERIA DE PROTECCIÓN DE DATOS.....	10
7. POLÍTICAS.....	11
8. FINALIDADES.....	16
9. MARCO LEGAL.....	18
10. DEBERES DEL RESPONSABLE DEL TRATAMIENTO.....	21
11. DERECHOS DE LOS TITULARES.....	22
12. AUTORIZACIÓN.....	23
13. ALMACENAMIENTO Y TRATAMIENTO DE LOS DATOS PERSONALES....	25
14. TRANSFERENCIAS Y TRANSMISIONES INTERNACIONALES DE DATOS PERSONALES.....	25
15. PROTECCIÓN DE DATOS PERSONALES EN SISTEMAS DE VIDEOVIGILANCIA, REGISTROS DE AUDIO O FOTOGRAFÍA.....	27
16. PROCEDIMIENTO PARA ATENCIÓN Y RESPUESTA A PETICIONES, CONSULTAS, QUEJAS Y RECLAMOS DE LOS TITULARES DE DATOS PERSONALES.....	30
17. PROTECCIÓN DE LOS DATOS PERSONALES.....	32
18. REPORTE DE INCIDENTES DE SEGURIDAD.....	32
19. REGISTRO NACIONAL DE BASES DE DATOS.....	38
20. VIGENCIAS.....	39
21. TABLA DE SEGUIMIENTO Y CONTROL.....	39



POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

1. JUSTIFICACIÓN

FUNDACIÓN SILARAA identificada con NIT 901.845.693–9 es una Fundación que tiene como objeto impulsar la educación, la ciencia y la tecnología, la protección del medio ambiente, la asociación profesional de médicos veterinarios y zootecnistas, el desarrollo social, la protección de los animales. Las Actividades Meritorias de la FUNDACIÓN corresponden a: 1. Promover el desarrollo de la ciencia y la tecnología en áreas de reproducción animal asistida en el país. 2. Actuar como capacitador de grupos profesionales de médicos veterinarios y zootecnistas, así como demás profesionales que participan en actividades de reproducción animal asistida. 3. Focalizar la educación Informal de profesionales de las áreas de reproducción animal a través del Simposio Latinoamericano de Reproducción Animal Asistida. 4. Investigación en áreas de la medicina veterinaria y en especial de la reproducción animal asistida y conexas. 5. Actividades de apoyo al cuidado de animales en condición de calle, y apoyo a albergues transitorios de para animales abandonados para adopción. 6. Actividades de esterilización de animales. 7. Actividades de protección al medio ambiente. Conservación, recuperación, protección, manejo, uso y aprovechamiento de los recursos naturales renovables y el medio ambiente sostenible. 8. Actividades de concientización y sensibilización del cuidado del medio ambiente y cuidado de animales. 9. Actividades de desarrollo empresarial. Promoción del desarrollo empresarial y el emprendimiento definido por la Ley 1014 de 2006. 10. Promoción y apoyo a entidades sin ánimo de lucro que ejecuten acciones directas en el territorio nacional en alguna de las actividades meritorias descritas en este artículo. Para la obtención de recursos que garanticen ingresos y activos para el cumplimiento de su objeto social, la FUNDACIÓN también podrá desarrollar las siguientes actividades: 1. Prestación de servicios médicos veterinarios en todo el país. 2. Importar y exportar productos de medicina veterinaria. 3. Realizar actividades de asesoría y consultoría en medio ambiente, medicina veterinaria, cuidado animal, derechos humanos, desarrollo científico. 4. Comercializar productos para el cuidado personal, el cuidado animal, el cuidado de la naturaleza, el cuidado del medio ambiente, maquinaria industrial y de laboratorios, insumos médico veterinarios, alimentación de humanos y de personas. 5. Desarrollar actividades logísticas y apoyo de eventos. 6. Desarrollar actividades de asistencia gerencial a entidades públicas y privadas. 7. Adquirir, enajenar y recibir, a cualquier título, toda clase de bienes, muebles e inmuebles, instalaciones, maquinaria o mercaderías y otros implementos o activos destinados al funcionamiento y explotación de empresas, comerciales o de servicios, celebrar negocios sobre estos, tales como arrendarlos, administrarlos, gravarlos, prestarlos, importarlos, exportarlos y enajenarlos. 8. Promover o constituir sociedades y otras personas jurídicas o empresas, cualquier sea su naturaleza u objeto o el tipo de vinculación a ellas, con o sin ánimo de lucro, mediante la adquisición o suscripción de acciones, partes o



cuotas de interés social o haciendo aportes de cualquier especie. 9. Obtener, adquirir, poseer y explotar concesiones, privilegios, invenciones, patentes, nombres comerciales, marcas, secretos industriales, licencias y otros derechos constitutivos de propiedad industrial, la concesión de su explotación a terceros, así como la adquisición de concesiones para su explotación. 10. Invertir en bienes muebles o inmuebles, efectuar su negociación, venta, permuta, gravamen, arrendamiento o cualquier otra negociación sobre los mismos, y promover o ejecutar todos los negocios relacionados con finca raíz, tales como construcción de edificaciones. 11. Efectuar negocios jurídicos sobre toda clase de títulos valores, tales como girarlos, aceptarlos, endosarlos, cobrarlos y pagarlos. 12. Intervenir en operaciones de crédito como la celebración de contratos de mutuo y otras operaciones financieras, con o sin interés, dando o recibiendo las garantías del caso, sin que ello llegué a configurar intermediación financiera. 13. Constituir cauciones reales o personales en garantía de obligaciones que contraiga la FUNDACIÓN. 14. Invertir sus fondos o disponibilidades, en activos financieros o valores mobiliarios tales como títulos emitidos por instituciones financieras o entidades públicas, cédulas hipotecarias, títulos valores, bonos, así como su negociación, venta, permuta o gravamen. 15. Participar en licitaciones y concursos públicos y privados o en contrataciones directas. 16. Celebrar todo tipo de alianzas y convenios con entidades públicas y privadas. 17. Celebrar acuerdos de cooperación nacional o internacional, técnica y financiera y obrar como filiar o corresponsal de entidades de desarrollo. 18. Promover investigaciones y estudios de cualquier naturaleza y materia, ya sea directamente o a través de entidades especializadas, recibir y efectuar donaciones o contribuciones con fines científicos, culturales o de desarrollo social del país. 19. Cooperar con independencia en las iniciativas de competitividad y de desarrollo integral del Gobierno Nacional y de los Gobierno Departamentales y Municipales, articulando proyectos con organizaciones públicas y privadas. 20. Celebrar contratos de trabajo, transporte, seguros, de cuentas en participación, realizar operaciones de comercio nacional e internacional, así como representar, agenciar y distribuir toda clase de bienes y servicios, relacionados con el objeto principal, realizar o prestar asesorías y en general, celebrar, ejecutar, desarrollar y llevar a término todos aquellos actos o contratos que se relacionen con el objeto principal. 21. Realizar cualquier otro acto o contrato necesario o conveniente para el desarrollo de su objeto, o que de una u otra manera se relacione directamente con él, y los que tengan como finalidad ejercer los derechos o cumplir las obligaciones legales o convencionalmente derivadas de la existencia y funcionamiento de la FUNDACIÓN.

2. OBJETIVO

El presente manual contentivo de la Política de Privacidad y Protección de Datos Personales (en adelante “Política de Privacidad”) es dar cumplimiento a la Ley Estatutaria 1581 de 2012, su Decreto Reglamentario 1074 de 2015 (Capítulo 25) y demás normas que rigen la protección de datos personales, o aquellas que las



complementen, sustituyan, modifiquen o deroguen y en especial, garantizar el Derecho de Habeas Data de los Titulares de datos personales.

3. ALCANCE

La presente Política de Privacidad es aplicable tanto a **FUNDACIÓN SILARAA**, en calidad de responsable del tratamiento y a sus empleados directos e indirectos, como a todas aquellas terceras personas naturales o jurídicas a quienes transmita o transfiera datos personales de los Titulares que comprenden los grupos de interés del Responsable del tratamiento, cuando estos realicen algún tratamiento sobre los mismos.

4. PRINCIPIOS

FUNDACIÓN SILARAA en cumplimiento de lo dispuesto en el TÍTULO II PRINCIPIOS RECTORES de la ley 1581 de 2012, aplicará los siguientes principios rectores en materia de protección de datos personales, los cuales constituyen las reglas a seguir en el tratamiento de datos personales que realicen el Responsable del tratamiento, sus empleados y todas aquellas terceras personas naturales o jurídicas a quienes transmita o transfiera datos personales de los Titulares que comprenden sus grupos de interés, cuando estos realicen algún tratamiento sobre los mismos:

- a) **Principio de legalidad:** el tratamiento de datos personales es una actividad reglada que debe sujetarse a lo establecido en la Constitución Política de Colombia, en la ley, en el presente Manual de Política de Privacidad y en las demás disposiciones que complementen o desarrollen.
- b) **Principio de finalidad:** el tratamiento de los datos personales debe obedecer a una finalidad legítima de acuerdo con la Constitución Política de Colombia y la ley, la cual debe ser informada al Titular.
- c) **Principio de libertad:** el tratamiento solo puede llevarse a cabo 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. Quedan exceptuados de este principio los datos públicos, los cuales podrán ser objeto de tratamiento sin que se requiera autorización del Titular, conforme a lo dispuesto por la Ley 1581 de 2012 y su Decreto Reglamentario 1074 de 2015.
- d) **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.

- e) **Principio de transparencia:** en el tratamiento debe garantizarse el derecho del Titular a obtener en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.
- f) **Principio de acceso y circulación restringida:** el tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de ley vigentes y la Constitución Política de Colombia. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, excepto que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los Titulares o terceros autorizados.
- g) **Principio de seguridad:** la información sujeta a tratamiento se deberá proteger mediante el uso de 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.
- h) **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.

5. DEFINICIONES

Se establecen las siguientes definiciones dentro de la presente política, las demás se entenderán en su sentido natural y lógico:

- a) **CCTV:** Circuito cerrado de televisión (Closed Circuit Television), es un sistema de vigilancia por medio de video para fines de control de actividades, supervisión de áreas, personal, controles de seguridad.
- b) **Datos personales:** cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. La naturaleza de los datos personales puede ser pública, semiprivada, privada o sensible.
- c) **Dato privado:** “Es el dato que por su naturaleza íntima o reservada sólo es relevante para el Titular”.

- d) **Dato semiprivado:** “Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV” de la Ley 1266.
- e) **Dato público:** “Es el dato calificado como tal según los mandatos de la Ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados”, de conformidad con la Ley 1266 de 2008. “Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas”.

Conforme a la Ley 1581 de 2012 establece las siguientes categorías especiales de datos personales:

- f) **Datos sensibles:** Son “aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos”.

La Ley 1581 de 2012 prohíbe el tratamiento de datos sensibles con excepción de los siguientes casos:

- (i) Cuando la información es requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- (ii) Cuando el Titular otorga su consentimiento;
- (iii) Casos de urgencia médica o sanitaria;
- (iv) Cuando se trata de datos relacionados con el Registro Civil;
- (v) El Tratamiento es necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado;
- (vi) El tratamiento es 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;
- (vii) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y;

- (viii) El Tratamiento tenga una finalidad histórica, estadística o científica, en este último caso deben adoptarse las medidas conducentes a la supresión de identidad de los Titulares.
- g) **Datos personales de los niños, niñas y adolescentes:** Se debe tener en cuenta que aunque la Ley 1581 de 2012 prohíbe el tratamiento de los datos personales de los niños, niñas y adolescentes, salvo aquellos que por su naturaleza son públicos, la Corte Constitucional precisó que independientemente de la naturaleza del dato, se puede realizar el tratamiento de éstos “siempre y cuando el fin que se persiga con dicho tratamiento responda al interés superior de los niños, niñas y adolescentes y se asegure sin excepción alguna el respeto a sus derechos prevalentes”.
- h) **Niño o niña:** personas entre los 0 y 12 años (Código de la Infancia y la Adolescencia, artículo 3).
- i) **Adolescente:** personas entre 12 y 18 años de edad (Código de la Infancia y la Adolescencia, artículo 3).
- j) **Autorización:** consentimiento previo, expreso e informado del Titular de los datos personales para llevar a cabo el tratamiento de sus datos personales, la cual puede ser recolectada de manera (i) escrita, (ii) oral, (iii) mediante conductas inequívocas, que permitan concluir de manera razonable que este otorgó la autorización.
- k) **Aviso de privacidad:** documento físico, electrónico o en cualquier otro formato generado por el Responsable del tratamiento, que se pone a disposición del Titular para el tratamiento de sus datos personales. En el aviso de privacidad se 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.
- l) **Base de datos:** conjunto organizado de datos personales físico o electrónico (digital) que sea objeto de tratamiento manual o automatizado.
- m) **Titular:** para los efectos de la Ley 1266 de 2008, es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del Derecho de Habeas Data y demás derechos y garantías consagrados en dicha ley y las normas que la complementen, modifiquen, sustituyan o deroguen. Para los efectos de la Ley 1581 de 2012, es la persona natural cuyos datos personales sean objeto de tratamiento.
- n) **Transferencia:** la transferencia de datos tiene lugar cuando el Responsable y/o Encargado del tratamiento de datos personales, ubicado en Colombia,

envía la información o los datos personales a un receptor, que a su vez es Responsable del tratamiento y se encuentra dentro o fuera del país.

- o) Transmisión:** tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.
- p) Transmisión internacional de datos:** Las transmisiones internacionales de datos personales que se efectúen entre un Responsable y un Encargado para permitir que el encargado realice el tratamiento por cuenta del responsable, no requerirán ser informadas al Titular ni contar con su consentimiento cuando exista un contrato en los términos del artículo 2.2.2.25.5.2. (Decreto 1377 de 2013, arto 24)
- q) Tratamiento:** cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, actualización, uso, circulación, transferencia, transmisión o supresión.
- r) Derecho de Habeas Data:** conforme a lo dispuesto por el artículo 15 de la Constitución Política de Colombia, es el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
- s) RNBD:** Registro Nacional de Base de datos es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país; y que será de libre consulta para los ciudadanos, de acuerdo con la normatividad que para tal efecto expida el Gobierno Nacional
- t) Finalidad de base de datos:** el tratamiento de los datos personales debe obedecer a una finalidad legítima de acuerdo con la Constitución Política de Colombia y la ley, la cual debe ser informada al Titular.
- u) Responsable de 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”. La Superintendencia de Industria y Comercio, de acuerdo con la ley es Responsable de Tratamiento de datos personales contenidos en sus bases de datos,
- v) 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”. **FUNDACIÓN SILARAA** podrá realizar el tratamiento de sus datos personales a través de Encargados.

- w) **Oficial de protección de datos:** Corresponde a la persona designada a una persona o área que "asuma la función de protección de datos personales" y que "dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y el presente decreto (Art. 23 decreto 1377 de 2013, compilado en decreto 1074 de 2015).

6. ROLES EN MATERIA DE PROTECCIÓN DE DATOS

Para los efectos del presente Manual de Política de tratamiento de datos personales, se definen los siguientes roles al interior de la Entidad

- a) **Administrador de base de datos personales:** Funcionario o Encargado que tiene a cargo y realiza tratamiento a una o más bases de datos que tiene información personal, corresponderá a Dirección Ejecutiva o Dirección Operativa.
- b) **Oficial de protección de datos:** La Dirección Ejecutiva designará un abogado, administrador de empresas o profesional de área afín a las anteriores, quien ejercerá el rol de oficial de datos, quien cumplirá las siguientes funciones:
- Dar trámite a las solicitudes de tratamiento de datos personales.
 - Velar por la implementación efectiva de las políticas y procedimientos adoptados por ésta para cumplir las normas.
 - Velar por que se adelante la implementación de buenas prácticas de gestión de datos personales dentro de la empresa.
 - Estructurar, diseñar y administrar el programa que permita a la organización cumplir las normas sobre protección de datos personales.
 - Establecer los controles de ese programa, su evaluación y revisión permanente de las políticas y procedimientos de protección de datos al interior de la empresa.
 - Promover la elaboración e implementación de un sistema que permita administrar los riesgos del tratamiento de datos personales.
 - Coordinarla definición e implementación de los controles de la Política de Tratamiento de Datos Personales y Programa Integral de Gestión de datos Personales.
 - Servir de enlace y coordinador con las demás áreas de la organización para asegurar una implementación transversal de la Política de Tratamiento de Datos Personales y Programa Integral de Gestión de datos Personales.
 - Impulsar una cultura de protección de datos dentro de la organización.

- Mantener un inventario de las bases de datos personales en poder de la organización y clasificarlas según su tipo.
 - Registrar las bases de datos de la organización en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la SIC.
 - Obtener las declaraciones de conformidad de la SIC cuando sea requerido.
 - Revisar los contenidos de los contratos de transmisiones internacionales de datos que se suscriban con Encargados no residentes en Colombia.
 - Analizar las responsabilidades de cada cargo de la organización, para diseñar un programa de entrenamiento en protección de datos personales específico para cada uno de ellos
 - Realizar un entrenamiento general en protección de datos personales para todos los empleados de la compañía.
 - Realizar el entrenamiento necesario a los nuevos empleados, que tengan acceso por las condiciones de su empleo, a datos personales gestionados por la organización.
 - Integrar las políticas de protección de datos dentro de las actividades de las demás áreas de la organización (talento humano, seguridad, call centers y gestión de proveedores, etc.).
 - Medir la participación, y calificar el desempeño, en los entrenamientos de protección de datos.
 - Requerir que, dentro de los análisis de desempeño de los empleados, se encuentre haber completado satisfactoriamente el entrenamiento sobre protección de datos personales.
 - Velar por la implementación de planes de auditoría interna para verificar el cumplimiento de sus políticas de tratamiento de la información personal.
 - Acompañar y asistir a la organización en la atención de las visitas y los requerimientos que realice la Superintendencia de Industria y Comercio.
 - Realizar seguimiento la Política de Tratamiento de Datos Personales y en caso de adoptarse al Programa Integral de Gestión de datos Personales.
- c) **Responsable:** Será responsable de la Política de Privacidad la **FUNDACIÓN SILARAA**, representada por su Director, quien contará con apoyo de un profesional de la oficina asesora jurídica para el adecuado manejo de la Política.

7. POLÍTICAS

Se establecen las siguientes directrices generales:



Primero: Cumplir con toda la normatividad legal vigente colombiana que dicte disposiciones para la protección de datos personales.

Segundo: Cumplir con la ley de protección de datos personales de acuerdo con lo contemplado en el Manual de Gobierno Corporativo de **FUNDACIÓN SILARAA**.

Tercero: Los responsables y encargados del tratamiento de datos personales serán responsables de las faltas que se llegaren a generar por violación a la presente política de tratamiento de datos personales.

Cuarto: Las Políticas específicas relacionadas con el tratamiento de Datos Personales:

- a) **FUNDACIÓN SILARAA** realiza el tratamiento de Datos Personales con la debida autorización por medio de un documento físico, electrónico, mensaje de datos, Internet, sitio web, o también de manera verbal o telefónica o en cualquier otro formato que permita su posterior consulta a fin de constatar de forma inequívoca que sin el consentimiento del titular los datos nunca hubieran sido capturados y almacenados en medios electrónicos o físicos. Así mismo se podrá obtener por medio de conductas claras e inequívocas del Titular que permitan concluir de una manera razonable que este otorgó su consentimiento para el manejo de sus Datos Personales.
- b) **FUNDACIÓN SILARAA** solicitará la autorización a los Titulares de los datos personales y mantendrá las pruebas de ésta.
- c) Toda labor de tratamiento de Datos Personales realizada por **FUNDACIÓN SILARAA** deberá corresponder a la legalmente obtenida en el giro ordinario de su objeto social y que se relacionan con el cumplimiento de su objeto social, así como de las actividades económicas para las cuales fue creada, y que especialmente vinculan:
 - Propiedad industrial.
 - Desarrollo del objeto social de la Fundación
 - Protección al consumidor.
 - Contratos de Laborales.
 - Contratos de Prestación de servicios personales y/o profesionales.
 - Contratos Administrativos.
 - Contratos para la adquisición de bienes y servicios.
 - Contratos de usuarios de procesos de reproducción animal asistida o por embriones.
 - Asuntos judiciales.
 - Información contable, tributaria y financiera.
 - Información societaria.



- d) El Dato Personal sometido a Tratamiento deberá ser veraz, completo, exacto, actualizado, comprobable y comprensible. **FUNDACIÓN SILARAA** mantendrá la información bajo estas características siempre y cuando el titular informe oportunamente sus novedades.
- e) Los Datos Personales solo serán Tratados por aquellos trabajadores que cuenten con el permiso para ello, o quienes dentro de sus funciones tengan a cargo la realización de tales actividades o por los Encargados.
- f) **FUNDACIÓN SILARAA** autorizará expresamente al Administrador de las bases de datos para realizar el tratamiento solicitado por el Titular de la información.
- g) **FUNDACIÓN SILARAA** no hará disponibles Datos Personales para su acceso a través de Internet u otros medios masivos de comunicación, a menos que se trate de información pública o que se establezcan medidas técnicas que permitan controlar el acceso y restringirlo solo a las personas autorizadas por ley o por el titular.
- h) Todo Dato Personal que no sea Dato Público se tratará por **FUNDACIÓN SILARAA** como confidencial, aun cuando la relación contractual o el vínculo contractual, entre el Titular del Dato Personal y **FUNDACIÓN SILARAA** haya finalizado, salvo cuando exista autorización para la transferencia y transmisión del dato por el Titular, o el mismo sea requerido a través de orden administrativa o judicial y hasta la eliminación del dato, luego de cumplida su utilidad. A la terminación de dicho vínculo, tales Datos Personales deben continuar siendo Tratados de acuerdo con lo dispuesto en las políticas de gestión documental de **FUNDACIÓN SILARAA**.
- i) Cada área de **FUNDACIÓN SILARAA** debe evaluar la pertinencia de anonimizar los documentos de carácter público que contengan datos personales, para su publicación.
- j) El Titular, directamente o a través de las personas debidamente autorizadas, podrá consultar sus Datos Personales en todo momento y especialmente cada vez que existan modificaciones en las Políticas de Tratamiento de la información.
- k) **FUNDACIÓN SILARAA** suministrará, actualizará, ratificará o suprimirá los Datos personales a solicitud del Titular para corregir información parcial, inexacta, incompleta, fraccionada que induzca al error o aquella que haya sido tratada previa a la vigencia de la ley y que no tenga autorización o sea prohibida.



- l) Cuando le sea solicitada información, ya sea mediante una petición, consulta o reclamo por parte del Titular, sobre la manera como son utilizados sus Datos Personales, **FUNDACIÓN SILARAA** deberá entregar dicha información.
- m) A solicitud del Titular y cuando no tenga ningún deber legal o contractual de permanecer en las bases de datos de **FUNDACIÓN SILARAA**, los Datos Personales deberán ser eliminados. En caso de proceder una revocatoria de tipo parcial de la autorización para el Tratamiento de Datos Personales para algunas de las finalidades **FUNDACIÓN SILARAA** podrá seguir utilizando los datos para las demás finalidades respecto de las cuales no proceda dicha revocatoria.
- n) Las políticas establecidas por **FUNDACIÓN SILARAA** respecto al tratamiento de Datos Personales podrán ser modificadas en cualquier momento. Toda modificación se realizará con apego a la normatividad legal vigente, y las mismas entrarán en vigencia y tendrán efectos desde su publicación a través de los mecanismos dispuestos por la SIC para que los titulares conozcan la política de tratamiento de la información y los cambios que se produzcan en ella.
- o) Los Datos Personales solo podrán ser tratados durante el tiempo y en la medida que la finalidad de su tratamiento lo justifique.
- p) **FUNDACIÓN SILARAA** será más rigurosa en la aplicación de las políticas de tratamiento de la información cuando se trate del uso de datos personales de los niños, niñas y adolescentes asegurando la protección de sus derechos fundamentales.
- q) **FUNDACIÓN SILARAA** podrá intercambiar información de Datos Personales con autoridades gubernamentales o públicas tales como autoridades administrativas, de impuestos, organismos de investigación y autoridades judiciales, cuando la soliciten en ejercicio de sus funciones.
- r) Los Datos Personales sujetos a tratamiento deberán ser manejados proveyendo para ello todas las medidas tanto humanas como técnicas para su protección, brindando la seguridad de que ésta no pueda ser copiada, adulterada, eliminada, consultada o de alguna manera utilizada sin autorización o para uso fraudulento.
- s) Cuando finalice alguna de las labores de tratamiento de Datos Personales por los Servidores, contratistas o Encargados del tratamiento, y aun después de finalizado su vínculo o relación contractual con **FUNDACIÓN SILARAA**, éstos están obligados a mantener la reserva de la información de acuerdo con la normatividad vigente en la materia.



- t) **FUNDACIÓN SILARAA** divulgará en sus servidores, contratistas y terceros encargados del tratamiento las obligaciones que tienen en relación con el tratamiento de Datos Personales mediante campañas y actividades de orden pedagógico.
- u) **FUNDACIÓN SILARAA** no realizará transferencia de información relacionada con Datos Personales a países que no cuenten con los niveles adecuados de protección de datos, de acuerdo con los estándares que estén fijados en la Superintendencia de Industria y Comercio SIC.
- v) El Titular de los datos personales puede ejercer, principalmente, sus derechos mediante la presentación de consultas y reclamos ante **FUNDACIÓN SILARAA**, en su sede cuyo domicilio es la Carrera 14 No. 77 A - 49 de Bogotá D.C., y por el correo electrónico siralaa24@gmail.com
- w) El Titular de los datos personales puede ejercer, principalmente, sus derechos mediante la presentación de quejas ante la SIC, en su sede cuyo domicilio es la carrera 13 No. 27 – 00 piso 1 y 3, y por el correo electrónico contactenos@sic.gov.co.
- x) Cuando exista un Encargado del Tratamiento de Información de Datos Personales, **FUNDACIÓN SILARAA** deberá garantizar que la información que le suministra sea veraz, completa, exacta, actualizada, comprobable y comprensible.

Adicionalmente le comunicará de manera oportuna todas las novedades a que haya lugar para que la información siempre se mantenga actualizada.

- a) En el caso de existir un Encargado del Tratamiento de información de Datos Personales, **FUNDACIÓN SILARAA** suministrará según el caso, información de Datos Personales únicamente con la autorización del Titular.
- b) **FUNDACIÓN SILARAA** registrará las bases de datos en el Registro Nacional de Base de Datos - RNBD, en cumplimiento a lo establecido en la Ley 1581 de 2012.
- c) Los Jefes de Oficina reportarán las bases de datos con información personal que administren e informarán las novedades de su administración al Gestor. Igualmente, deberán reportar las nuevas bases de datos que se constituyan.
- d) **FUNDACIÓN SILARAA** implementará procedimientos para garantizar el cumplimiento de sus políticas de tratamiento de la información personal.
- e) El incumplimiento de las políticas de tratamiento de la información acarreará las sanciones contempladas en el Manual de Gobierno Corporativo, Códigos



de Ética, Reglamento Interno de Trabajo y demás instrumentos legales y corporativos que se adopten al interior de la empresa.

- f) Los trabajadores y contratistas que tengan archivos y bases de datos pertenecientes al ámbito personal o doméstico en los equipos de cómputo de la entidad, deberán mantener dicha información en una carpeta que sea identificable, de manera inequívoca, que es de su uso personal.
- g) **FUNDACIÓN SILARAA** implementará el aviso de privacidad al momento de recolectar datos personales.
- h) **FUNDACIÓN SILARAA** deberá consignar de manera clara y expresa en cada contrato o documento que implique recolección o incorporación de información o datos personales, las correspondientes autorizaciones para el tratamiento de datos personales.
- i) **FUNDACIÓN SILARAA**, deberá acogerse a las minutas o documentos tipos de autorización de tratamiento de datos personales adjuntos al presente documento en caso de que no se pueda suplir en contrato o medio diferente dicho documento en los términos del literal anterior.
- j) **FUNDACIÓN SILARAA** deberá publicar la presente política de tratamiento de datos personales en el portal Web que cree o adopte.

8. FINALIDADES

Para los efectos de la presente Política de Privacidad, el Responsable del tratamiento directamente o a través del Encargado del tratamiento, podrá recolectar, almacenar, usar, circular, actualizar, suprimir o realizar cualquier otro tipo de tratamiento sobre los datos personales de sus grupos de interés, ajustándose en todo momento a lo dispuesto por las normas vigentes y para las finalidades que se describen a continuación:

- a) Efectuar las gestiones pertinentes para el desarrollo del objeto social de la compañía en lo que tiene que ver con el cumplimiento del objeto del contrato celebrado con el Titular de la información.
- b) Realizar invitaciones a eventos, reuniones, juntas y ofrecer productos y servicios.
- c) Gestionar trámites (solicitudes, quejas, reclamos).
- d) Realizar acciones de inteligencia de negocios, realizar procesos de recolección, tratamiento, transformación y análisis de grandes volúmenes de

datos -big data-, creación de propuestas a la medida, prospectiva y analítica, investigación y tendencias de preferencias o de mercado; identificar trazabilidad y patrones de consumo con fines estadísticos; entendimiento de perfiles, rutas de navegación, seguimiento de preferencias y demás comportamientos del titular de tratamiento de datos.

- e) Formular o ejecutar proyectos, programas sociales, educativos, análisis estadísticos, encuestas, diagnósticos de problemáticas, estudios sociales, estudios ambientales y de impacto ambiental, análisis sectoriales, estudios socioeconómicos, estudios demográficos, estudios de urbanización o zonificación, estudios de género, estudios a población vulnerable o en condición de discapacidad, estudios a población desplazada, desmovilizada o reinsertada, procesos de formación, capacitación o sensibilización, entre otros.
- f) Efectuar encuestas de satisfacción respecto de los bienes y servicios ofrecidos por **FUNDACIÓN SILARAA**.
- k) Suministrar información de contacto a la fuerza comercial y/o red de proveedores, distribución, telemarketing, investigación de mercados y cualquier tercero con el cual **FUNDACIÓN SILARAA** actuará como Responsable del Tratamiento, tenga un vínculo contractual para el desarrollo de actividades de ese tipo o para la ejecución de las mismas.
- l) Contactar al Titular a través de medios telefónicos para realizar encuestas, estudios y/o confirmación de datos personales necesarios para la ejecución de una relación contractual.
- m) Contactar al Titular a través de medios electrónicos – SMS o chat para el envío de noticias relacionadas con campañas de fidelización o mejora de servicio.
- n) Contactar al Titular a través de correo electrónico para el envío de extractos, estados de cuenta o facturas en relación con las obligaciones derivadas del contrato celebrado entre las partes.
- o) Dar cumplimiento a las obligaciones contraídas por **FUNDACIÓN SILARAA** con el Titular de la Información, con relación al pago de salarios, prestaciones sociales y demás retribuciones consagradas en el contrato de trabajo o según lo disponga la ley.
- p) Ofrecer programas de bienestar corporativo y planificar actividades empresariales, para el titular y sus beneficiarios hijos, cónyuge, compañero permanente.



- q) Prestar los servicios ofrecidos por **FUNDACIÓN SILARAA** y aceptados en el contrato suscrito.
- r) Suministrar la información a terceros con los cuales **FUNDACIÓN SILARAA** tenga relación contractual y que sea necesario entregársela para el cumplimiento del objeto contratado.
- s) Transmitir datos a terceros en el marco de estrategias de marketing por medios digitales, audiovisuales, streaming, redes sociales, Word-of-Mouth Marketing (WOM), páginas sociales, y demás que utilice **FUNDACIÓN SILARAA**, para que difunda la información personal tal como nombre, imagen personal, marca, ganaderías, voz y video y demás información que recaude el autorizado de manera legal en el marco del presente contrato, y en las que cuya autorización de Tratamiento de Datos se informe dicha finalidad.
- t) Transferir datos personales fuera del país a socios o accionistas, filiales o matrices de **FUNDACIÓN SILARAA** para cumplir con las regulaciones anti lavado de activos que le aplican.
- u) Transferir datos personales fuera del país a socios o accionistas, filiales, matrices o franquiciadores de **FUNDACIÓN SILARAA** para realizar procesos de control, vigilancia, o capacitación internacional en materia de formación científica, técnica o profesional relacionada con el objeto social de la compañía.
- v) Transferir datos personales de los trabajadores fuera del país a socios o accionistas, filiales o matrices de **FUNDACIÓN SILARAA** para realizar trámites de autorizaciones de permisos especiales, visados y demás trámites migratorios que permitan ejecutar labores fuera del territorio nacional.
- w) Transferir datos personales de los trabajadores fuera del país a las autoridades públicas o administrativas que lo requieran para gestionar permisos o autorizaciones.
- x) Transmitir los datos personales fuera del país a terceros con los cuales **FUNDACIÓN SILARAA** haya suscrito un contrato de procesamiento de datos y sea necesario entregársela para el cumplimiento del objeto contractual.

9. MARCO LEGAL

La presente Política de Tratamiento de Datos se encuentra comprendida dentro del siguiente marco normativo:

Constitución Política, artículo 15.



“ARTÍCULO 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.

Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.”

Ley 1266 de 2008

“Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”

Ley 1581 de 2012

La Ley 1581 de 2012 desarrolla el derecho constitucional a conocer, actualizar y rectificar la información recogida en bases de datos y los demás derechos, libertades y garantías a que se refieren los artículos 15 y 20 de la Constitución (derecho a la intimidad y derecho a la información, respectivamente).

La citada ley se aplica a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por parte de entidades públicas o privadas.

Considerando el modo de conservación de una base de datos, se puede distinguir entre bases de datos automatizadas y bases de datos manuales o archivos.

Las bases de datos automatizadas son aquellas que se almacenan y administran con la ayuda de herramientas informáticas.

Las bases de datos manuales o archivos son aquellas cuya información se encuentra organizada y almacenada de manera física, como las fichas de



pedidos a proveedores que contengan información personal relativa al proveedor, como nombre, identificación, números de teléfono, correo electrónico, etc.

La ley exceptúa del régimen de protección (i) los archivos y las bases de datos pertenecientes al ámbito personal o doméstico; (ii) los que tienen por finalidad la seguridad y la defensa nacionales, la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo, (iii) los que tengan como fin y contengan información de inteligencia y contrainteligencia, (iv) los de información periodística y otros contenidos editoriales, (v) los regulados por la Ley 1266 de 2008 (información financiera y crediticia, comercial, de servicios y proveniente de terceros países) y (vi) los regulados por la Ley 79 de 1993 (sobre censos de población y vivienda).

Decretos Reglamentarios 1727 de 2009 y 2952 de 2010

Decreto 1727 de 2009: “por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información.”

Decreto 2952 de 2010: “Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008.”

Decreto Reglamentario parcial 1377 de 2013

“Por el cual se reglamenta parcialmente la Ley 1581 de 2012”.

Este decreto reglamenta en particular los procedimientos de recolección de datos personales, autorización para el tratamiento de datos personales y sensibles, la forma en la que se pueden obtener, la revocatoria de dicha autorización, lo relacionado con las políticas de tratamiento de datos, el ejercicio del derecho de los titulares, las limitaciones frente a la transferencia y transmisiones internacionales de datos personales, la responsabilidad demostrada frente al tratamiento de datos personales, y demás aspectos relacionados.

Decreto 1074 de 2015

“Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.”

Este decreto compila y regula aspectos especiales frente al tratamiento de la información, estableciendo que las entidades privadas y públicas receptoras de información deberán utilizar los datos e información solo para los fines aquí



establecidos y estarán obligadas a adoptar las medidas necesarias para garantizar su seguridad, circulación restringida y confidencialidad.

Decreto 886 de 2014

“Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.”

Este decreto tiene como objeto reglamentar la información mínima que debe contener el Registro Nacional de Bases de Datos, creado por la Ley 1581 de 2012, así como los términos y condiciones bajo las cuales se deben inscribir en este los Responsables del Tratamiento.

10. DEBERES DEL RESPONSABLE DEL TRATAMIENTO

El Responsable del Tratamiento ha sido definido por la Ley 1581 de 2012 como la 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.

FUNDACIÓN SILARAA al tener generar de manera permanente relaciones entre sus vinculados y terceros tiene ineludiblemente la responsabilidad de administrar y tratar adecuadamente la información con datos personales, garantizando el cumplimiento de las normas que dicha materia se expidan, así como la intimidad y privacidad de las personas jurídicas y naturales vinculadas con la empresa.

Son deberes de los Responsables del Tratamiento y, por consiguiente, de **FUNDACIÓN SILARAA** los establecidos en el artículo 17 de la Ley 1581 de 2012:

- 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 citada 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 que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a éste 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 cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la citada 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 citada ley.
- k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la citada 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.
- n) 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.
- o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio”.

11. DERECHOS DE LOS TITULARES

La Ley 1581 de 2012 establece que los Titulares de los datos personales tendrán los siguientes derechos:

- a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.
- b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la citada ley.
- c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales.
- d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la citada ley y las demás normas que la modifiquen, adicionen o complementen.
- e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando **FUNDACIÓN SILARAA** haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a la ley y a la Constitución.
- f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

Adicionalmente, el Decreto reglamentario 1377 de 2013 define que los responsables deberán conservar prueba de la autorización otorgada por los Titulares de datos personales para el Tratamiento de los mismos.

12. AUTORIZACIÓN

No se podrán recolectar datos personales sin la autorización previa, expresa e informada del Titular del dato. La autorización se puede obtener por cualquiera de los modos -escrito, verbal, electrónico o conductas inequívocas- previstos en el artículo 7 del Decreto 1377 de 2013, pero se debe de conservar evidencia de esta y entregarle prueba de la autorización a la persona titular del dato en caso de que la solicite. **FUNDACIÓN SILARAA** debe solicitar autorización previa, expresa e informada a los Titulares de los datos personales sobre los que requiera realizar el



tratamiento. Autorización previa significa, que el consentimiento debe ser otorgado por el titular, a más tardar en el momento de la recolección de los datos personales.

Esta manifestación de voluntad del titular puede darse a través de diferentes mecanismos puestos a disposición por **FUNDACIÓN SILARAA.**, tales como:

- a) Por escrito, por ejemplo, diligenciando un formato de autorización, dentro de un contrato, dentro de una oferta de servicios, dentro de un Aviso de Privacidad, una Aceptación de Términos y Condiciones de la Política de Privacidad en internet o por cualquier medio escrito mecánico o digital.
- b) De forma oral, por ejemplo, en una conversación telefónica o en videoconferencia.
- c) Mediante conductas inequívocas que permitan concluir que otorgó su autorización, por ejemplo, a través de su aceptación expresa a los términos y condiciones de una actividad dentro de los cuales se requiera la autorización de los participantes para el tratamiento de sus datos personales.

En ningún caso **FUNDACIÓN SILARAA** asimilará el silencio del titular a una conducta inequívoca.

Las autorizaciones expresas dadas por el titular para el tratamiento de datos, deberán ser conservada por **FUNDACIÓN SILARAA** a efectos de que obren como prueba del consentimiento y para que el dato pueda ser tratado con posterioridad a su consentimiento, conforme a las finalidades con las cuales operó la recolección del dato.

Autorización informada significa que al momento de solicitar el consentimiento al titular, debe informársele claramente:

- a) Los datos personales que serán recolectados.
- b) La identificación y datos de contacto del responsable y del encargado del tratamiento.
- c) Las finalidades específicas del Tratamiento que se pretende realizar, es decir: cómo y para qué se va a hacer la recolección, uso y circulación de los datos personales.
- d) Cuáles son los derechos que tiene como titular de los datos personales; para el efecto ver el numeral 10 derechos de los titulares de los datos personales.
- e) 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.
- f) El canal idóneo de atención a solicitudes.
- g) Medio para consulta de la PPTDP



13. ALMACENAMIENTO Y TRATAMIENTO DE LOS DATOS PERSONALES

FUNDACIÓN SILARAA actuando en calidad de responsable del tratamiento de datos personales, para el adecuado desarrollo de sus actividades sociales, así como para el fortalecimiento de sus relaciones con terceros, recolecta, almacena, usa, circula y suprime datos personales correspondientes a personas naturales y/o jurídicas con quienes tiene o ha tenido relación, tales como, sin que la enumeración signifique limitación, trabajadores y familiares de éstos, exempleados, usuarios, clientes, proveedores, oferentes, aspirantes a una vacante de la compañía y visitantes.

Estos datos serán almacenados en servidores de la empresa que utilice cotidiana y permanentemente en el giro ordinario de su objeto social, donde se almacenarán bases de datos en forma de archivos de gestión, así como almacenamiento en servicios de nube (Cloud Computing) en cuyo caso, se tomarán en cuenta en consideración las características del proveedor, procurando que el mismo sea adecuado de acuerdo con sus necesidades, tanto en infraestructura como en el aspecto reputacional. Para ello, se analizarán los comentarios, experiencias de otros clientes y exigirá o realizará previamente pruebas de seguridad a la plataforma que se va a contratar.

Así mismo, se analizarán los riesgos en cada una de las etapas del ciclo del dato o flujo de información, desde su recolección, hasta su disposición final. Para ello, utilizará una metodología de gestión de riesgos, y se realizará el análisis correspondiente a fin de determinar si con base en el estudio de riesgos, la información personal que se entregará al proveedor de servicios en la nube requiere aislamiento de hardware, software y/o datos y así se exigirá dentro de los términos del contrato y los acuerdos de niveles de servicio, en este caso se designará un supervisor que podrá ser el oficial de datos de la empresa.

El almacenamiento de los datos recaudados y tratados serán almacenados por el término que se requiera para la gestión en la dependencia que lo haya recolectado, en todo caso, luego de cumplida la finalidad para la cual fue recolectado, el dato se eliminará dentro de los treinta (30) días siguientes. Igualmente, las imágenes y videos que recolecte **FUNDACIÓN SILARAA** a través de sus cámaras de seguridad serán conservados por **FUNDACIÓN SILARAA** por un tiempo máximo de treinta (30) días.

14. TRANSFERENCIAS Y TRANSMISIONES INTERNACIONALES DE DATOS PERSONALES



FUNDACIÓN SILARAA podrá revelar a sus compañías vinculadas a nivel mundial, los datos personales sobre los cuales realiza el tratamiento, para su utilización y tratamiento conforme a esta política de protección de datos personales.

Igualmente, **FUNDACIÓN SILARAA** previa autorización del titular o su representante, podrá entregar los datos personales a terceros no vinculados a la Fundación, cuando:

- a) Se trate de contratistas en ejecución de contratos para el desarrollo de las actividades de **FUNDACIÓN SILARAA**
- b) Por transferencia a cualquier título de cualquier línea de negocio con la que se relaciona la información
- c) Para realizar las pruebas y exámenes médicos de ingreso y egreso de sus aspirantes y empleados.
- d) Para determinar el nivel de alcohol de sus empleados, con el fin de determinar si sus empleados se encuentran en estado de ebriedad durante la jornada laboral, de conformidad con el procedimiento para realizar pruebas de alcoholimetría adoptado por la **FUNDACIÓN SILARAA**
- e) Por requerimiento judicial o de entidad gubernativa.

FUNDACIÓN SILARAA celebrará contratos de transmisión de datos, atendiendo lo contemplado en el Artículo 2.2.2.25.5.2. del decreto 1074 de 2015, conforme al cual, el contrato que suscriba el Responsable con los encargados para el tratamiento de datos personales bajo su control y responsabilidad señalará los alcances del tratamiento, las actividades que el encargado realizará por cuenta del responsable para el tratamiento de los datos personales y las obligaciones del Encargado para con el titular y el Responsable. Mediante dicho contrato el Encargado se comprometerá a dar aplicación a las obligaciones del Responsable bajo la política de Tratamiento de la información fijada por este y a realizar el Tratamiento de datos de acuerdo con la finalidad que los Titulares hayan autorizado y con las leyes aplicables.

De modo que en aquellos casos en que el almacenamiento en la nube sea mediante la transmisión, debe celebrarse un contrato de transmisión de datos personales entre el responsable y el encargado de los datos objeto del contrato y deberá sujetarse a lo preceptuado en el artículo anteriormente reseñado.

En todo caso, en los contratos de transmisión de datos personales, que se suscriban entre **FUNDACIÓN SILARAA** y los encargados para el tratamiento de datos personales, se exigirá que la información sea tratada conforme a esta Política de Privacidad y se incluirán las siguientes obligaciones en cabeza del respectivo encargado:

- a) Dar tratamiento, a nombre de **FUNDACIÓN SILARAA** a los datos personales conforme los principios que los tutelan.



- b) Salvaguardar la seguridad de las bases de datos en los que se contengan datos personales.
- c) Guardar confidencialidad respecto del tratamiento de los datos personales.

15. PROTECCIÓN DE DATOS PERSONALES EN SISTEMAS DE VIDEOVIGILANCIA, REGISTROS DE AUDIO O FOTOGRAFÍA

Existen muchas condiciones de modo, lugar o situación en la que se toma u obtiene un registro fotográfico, de audio o de video (en redes sociales digitales, páginas web, un evento deportivo, un evento masivo, instituciones educativas, en la casa, en la calle, en un evento público, en el sitio de trabajo) o respecto de la persona fotografiada (un niño, una celebridad, un funcionario público, entre otras), las cuales merecen especial tratamiento de datos.

Solo aquellos registros de imagen, audio o video que contengan “cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables”, se considerarán como dato personal. Por eso, la foto será Dato Personal en la medida en que permita establecer la identidad de una o varias personas naturales en particular. Si, por ejemplo, la foto contiene la imagen de personas con máscaras en su rostro o que están de espaldas de tal forma que no se pueda establecer la identidad de cada una de ellas, pues esa fotografía no es un Dato Personal¹.

Cuando el registro de imagen o video captan la imagen de la cara de las personas u otras partes de su cuerpo que permiten identificarlas. Estas imágenes se consideran información biométrica. Los Datos Biométricos, a su vez, son un Dato Sensible tal y como se puede constatar en la definición legal del artículo 5 de la Ley Estatutaria 1581 de 2012. Los «datos biométricos»: incluyen información sobre las características físicas (rostro; huella dactilar; palma de la mano; retina; ADN) y “comportamentales” (forma de firmar, tono de voz) sobre las personas.

Los registros de imágenes y videos obtenidos por **FUNDACIÓN SILARAA** a través de sus cámaras de seguridad ubicadas en sus instalaciones, no serán utilizados para ninguna otra finalidad que el monitoreo y gestión de la seguridad a efectos de velar por la seguridad e identificar incidentes. Estas podrán ser entregadas ante las autoridades judiciales o administrativas como prueba de conductas indebidas o delitos que se cometan dentro de sus oficinas, instalaciones y/o vehículos, así como frente a la custodia y seguridad de sus bienes e información.

Únicamente las personas autorizadas por **FUNDACIÓN SILARAA** tienen acceso a las imágenes y videos recolectados a través de las cámaras de seguridad, quienes tendrán la obligación de cumplir con la presente política y de suscribir acuerdos de

¹ Guía para el Tratamiento de las Fotos como Datos Personales



confidencialidad, en caso de que sea implementado el sistema de videovigilancia. Para ello, se utilizarán señales o avisos distintivos en las zonas de videovigilancia, principalmente en las zonas de ingreso a los lugares que están siendo vigilados y monitoreados y al interior de estos, los avisos serán visibles y legibles teniendo en cuenta el lugar en el que opere el Sistema de Vigilancia, y corresponderán a los siguientes:



A en cumplimiento de la Ley 1581 de 2012 informa que, al ingresar, usted está siendo grabado por un circuito cerrado de grabación, con la finalidad de velar por la seguridad e identificar incidentes, el titular podrá ejercer sus derechos y presentar solicitudes relacionadas a través del correo **B**. Para mayor información consulte la Política de Tratamiento de Datos en la página: **C** o de forma presencial en las instalaciones administrativas de **D**. Al continuar con el ingreso, su conducta se tendrá como aceptación para el registro de las imágenes.

Convenciones:

A: Nombre de la empresa FUNDACIÓN SILARAA

B: Correo electrónico siralaa24@gmail.com

C: Página Web <https://silaraa.com/>

D: Dirección de la FUNDACIÓN SILARAA

De igual manera, en los casos en que se realice grabación de audio también se informará sobre dicha situación a los Titulares.

Los registros de imagen, audio o video que sean recolectados en eventos masivos, eventos cerrados, reuniones, eventos deportivos, capacitaciones o cualquier otro medio, en el cual participe **FUNDACIÓN SILARAA** como organizador o responsable del mismo, y sea éste responsable directamente de la obtención de los registros o delegue en particulares o estudios audiovisuales la obtención de dichos registros, deberá obtener previamente la obtención de la autorización de tratamiento de datos, para lo cual deberá acudir a cualquiera de los modos de obtención de autorización previstos en el artículo 7 del decreto 1377 de 2013, y que dentro de esta Política, se indican, sin limitarse a ellas, como:

- Autorización otorgada a través de planilla de asistencia.
- Banners, pendones o señalización visible en la cual se informe que el evento será grabado en audio, video o fotográfico, y en el que se exprese que la



permanencia o ingreso al mismo se entenderá como un permiso tácito, o conducta concluyente de la autorización.

- Se informe mediante interlocutor de manera previa que el evento o actividad contará con registro de audio, imagen o video y que la permanencia o ingreso al mismo se entenderá como un permiso tácito, o conducta concluyente de la autorización.

En los casos anteriores, deberá dejarse constancia fílmica, fotográfica o en audio del aviso indicado, el cual en todo caso deberá remitir a la Política de Privacidad y Tratamiento de Datos Personales que se encuentre en la Página Web de la Organización.

De igual manera, en los eventos en que se contrate a un tercero que recolecte datos personales a través de registros de audio, video y filmografía, deberá tener en cuenta que los datos personales **(i)** se obtuvieron lícitamente, ello implica que debe efectuar una debida diligencia sobre la procedencia de las fotos que no adquiere directamente del cliente o persona (Titular del Dato); y **(ii)** están autorizados a suministrarle a **FUNDACIÓN SILARAA** toda la información recolectada para usarla con fines específicos. No se debe olvidar que obtener fotografías “piratas”, “ilegales” o de dudosa procedencia puede dar lugar a responsabilidad administrativa ante la SIC, civil o penal.

El Titular de los datos personales también se encuentra facultado para solicitar la supresión de sus imágenes en la medida que no exista un deber legal o contractual que impida tal supresión, como sería por ejemplo el caso en que los datos personales recolectados mediante una grabación constituyan prueba de la presunta comisión de un delito. La solicitud de supresión, así como cualquier otra reclamación que se adelante ante los Responsables y Encargados del Tratamiento, deberá realizarse de acuerdo al procedimiento establecido por los artículos 15 y 16 de la Ley 1581 de 2012.

El Tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, de conformidad con lo establecido en el artículo 7 de la Ley 1581 de 2012 y cuando dicho Tratamiento cumpla con los siguientes parámetros y requisitos:

- a) Que responda y respete el interés superior de los niños, niñas y adolescentes;
- b) Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.



El registro de imágenes, audio o video de niños, niñas y adolescentes, será reservado, siendo los padres o representantes legales de los niños, niñas o adolescentes quienes podrán acceder a las imágenes de este. Así, en caso de que se pretenda dar acceso o circular imágenes de actividades o hechos donde aparezcan otros niños, niñas o adolescentes, se deberá solicitar la autorización de los padres o representantes legales de todos ellos.

En todo caso, el término de retención de las imágenes será limitado y razonable, en concordancia con la finalidad del Tratamiento de los datos recolectados.

Las imágenes, audios o videos que recolecte **FUNDACIÓN SILARAA** través de registros de y en eventos masivos, eventos cerrados, reuniones, eventos deportivos, capacitaciones o cualquier otro medio, en el cual participe **FUNDACIÓN SILARAA** como organizador o responsable del mismo, o para la formulación o ejecución de los proyectos, programas sociales, análisis estadísticos, encuestas, diagnósticos de problemáticas, estudios sociales, estudios ambientales y de impacto ambiental, análisis sectoriales, estudios socioeconómicos, estudios demográficos, estudios de urbanización o zonificación, estudios de género, estudios a población vulnerable o en condición de discapacidad, estudios a población desplazada, desmovilizada o reinsertada, procesos de formación, capacitación, sensibilización, entre otros serán conservados por **FUNDACIÓN SILARAA** sin limitación de tiempo, pudiendo en cualquier tiempo hacer uso de los mismos.

16. PROCEDIMIENTO PARA ATENCIÓN Y RESPUESTA A PETICIONES, CONSULTAS, QUEJAS Y RECLAMOS DE LOS TITULARES DE DATOS PERSONALES

Los titulares de los datos personales que estén siendo recolectados, almacenados, utilizados, puestos en circulación por **FUNDACIÓN SILARAA** podrán ejercer en cualquier momento sus derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.

Para el efecto, se seguirán siguientes parámetros establecidos, de conformidad con la Ley de Protección de Datos Personales:

El Titular o sus causahabientes, podrán solicitar a **FUNDACIÓN SILARAA**

- Información sobre los datos personales del titular que son objeto de tratamiento.
- Solicitar prueba de la autorización otorgada a **FUNDACIÓN SILARAA** para el tratamiento de sus datos personales.
- Información respecto del uso que se le ha dado por **FUNDACIÓN SILARAA** a sus datos personales.



Los medios habilitados para la presentación de peticiones y consultas son:

- Comunicación dirigida a **FUNDACIÓN SILARAA**, Carrera 14 No. 77 A - 49 de Bogotá D.C.
- Solicitud presentada al correo electrónico siralaa24@gmail.com

Las peticiones y consultas serán atendidas en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de las mismas o conforme a los términos establecidos en el artículo 14 de la ley 1581 de 2012.

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.

Atención y Respuesta a Quejas y Reclamos El titular o sus causahabientes, podrán solicitar a **FUNDACIÓN SILARAA**:

- La corrección o actualización de la información.
- La supresión de sus datos personales o la revocatoria de la autorización otorgada para el tratamiento de los mismos.
- Que se subsane o corrija el presunto incumplimiento a cualquiera de los deberes contenidos en la Ley de Protección de Datos Personales.

La solicitud deberá contener la descripción de los hechos que dan lugar a la queja o reclamo, la dirección y datos de contacto del solicitante y deberá acompañarse de los documentos que se quiera hacer valer.

Si la queja o reclamo se presentan incompletos, **FUNDACIÓN SILARAA** deberá requerir al interesado dentro de los diez (10) días siguientes a la recepción de la queja o reclamo para que subsane las fallas.

Transcurridos un (1) mes desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido de la queja o reclamo.

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 atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.



17. PROTECCIÓN DE LOS DATOS PERSONALES

FUNDACIÓN SILARAA en estricta aplicación del principio de seguridad en el tratamiento de datos personales, proporcionará 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.

La obligación y responsabilidad de **FUNDACIÓN SILARAA** se limita a disponer de los medios adecuados para este fin. **FUNDACIÓN SILARAA** exigirá a los proveedores de servicios que contrata, la adopción y cumplimiento de las medidas técnicas, humanas y administrativas adecuadas para la protección de los Datos Personales en relación con los cuales dichos proveedores actúen como Encargados.

Los datos personales recaudados serán confidenciales y reservados, y solo las personas autorizadas podrán tener acceso a la misma, y por ello se garantizará que los mismos sean depositados en los lugares que determine la Organización y excepcionalmente cuando los mismo se obtengan o administren a través de Encargados en las instalaciones de dichos responsables, y en sistema de almacenamiento de los computadores o discos externos del Responsable, o en sistema de nube, o cualquier otro medio de almacenamiento, estableciendo para cada caso en particular un procedimiento de identificación y autenticación de usuarios, controles de acceso físico y lógico y contraseñas robustas, que se cambiarán cada cierto tiempo, a efectos de procurar que terceros sin relación alguna con **FUNDACIÓN SILARAA** puedan tener acceso fraudulento a los mismos.

Para el traslado de los datos a terceros, se deberá garantizar condiciones de confidencialidad adecuadas. De no contar con anterioridad con la autorización de traslado de datos a terceros, en la Autorización de Tratamiento, se deberá comunicar al titular de dicho traslado.

FUNDACIÓN SILARAA deberá registrar y actualizar las bases de datos en el Registro Nacional de Base de Datos, así como suprimir aquellas que hayan cumplido los fines para los cuales fueron recaudadas.

18. REPORTE DE INCIDENTES DE SEGURIDAD

Los responsables del Tratamiento de Datos de **FUNDACIÓN SILARAA** deberán reportar el incidente de seguridad dentro los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o el área encargada de atenderlos. Independientemente del tamaño y complejidad del incidente de seguridad, todos los reportes deberán efectuarse a través del enlace previsto en la página web de la SIC.

Al efecto, **FUNDACIÓN SILARAA** deberá seguir los siguientes pasos para atender los incidentes de Seguridad:



Tomado de: Guía para la Gestión de Incidentes de Seguridad en el Tratamiento de Datos Personales -SIC-

01. Contener el Incidente de seguridad y hacer una evaluación preliminar:

Una vez que la **FUNDACIÓN SILARAA** tenga conocimiento de la ocurrencia de un incidente de seguridad deberá adoptar las medidas inmediatas para limitar esa falla y evitar cualquier compromiso adicional a la información de carácter personal bajo su cuidado.

En esta primera etapa, **FUNDACIÓN SILARAA** también deberá comenzar una investigación inicial sobre el evento u ocurrencia. La indagación preliminar ayudará a responder las siguientes preguntas respecto del incidente de seguridad:

- ¿Cómo se produjo?
- ¿Cuándo y dónde tuvo lugar?
- ¿Cuál es su naturaleza y quién lo detectó?
- ¿Se continúa compartiendo o divulgando información personal sin Autorización?
- ¿Quién tiene acceso a la información personal?
- ¿Qué se puede hacer para asegurar la información, detener el acceso, divulgación o disponibilidad no autorizada y reducir el riesgo de daños a los afectados?
- ¿Es un incidente de seguridad relacionado con Datos Personales que requiere la notificación a las personas tan pronto como sea posible?



Durante esta etapa preliminar, **FUNDACIÓN SILARAA** debe tener cuidado de no destruir la evidencia que pueda ser valiosa para:

- Establecer la causa del incidente de seguridad.
Identificar todos los riesgos generados a los Titulares de la información.
- Responder los requerimientos de la SIC u otras autoridades.

02. Evaluar los riesgos e impactos asociados con el Incidente de Seguridad

La adecuada gestión de riesgos requiere un profundo y juicioso proceso de identificación y evaluación del nivel de severidad del incidente de seguridad; la probabilidad de daño para los Titulares de la Información; el nivel de riesgo para sus derechos y libertades; y el Tratamiento que se dará a esos riesgos.

Un incidente de seguridad puede tener una variedad de efectos adversos sobre las personas que puede dar lugar a problemas de discriminación, suplantación de identidad o fraude, pérdidas financieras, daño reputacional, pérdida del carácter confidencial de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo. El nivel de riesgo del incidente de seguridad frente a los Titulares de la información puede ser cuantificado y/o calificado.

Tomando como referencia lo establecido para la Superintendencia de Industria y Comercio, según el nivel de impacto, el riesgo puede ser:

Bajo riesgo: es improbable que el incidente de seguridad tenga un impacto en las personas, y de generarlo, este sería mínimo.

Riesgo medio: el incidente de seguridad puede tener un impacto en las personas, pero es poco probable que el impacto sea sustancial.

Riesgo alto: el incidente de seguridad puede tener un impacto considerable en las personas afectadas.

Riesgo grave: el incidente de seguridad puede tener un impacto crítico, extenso o peligroso en las personas afectadas.

Se debe tener en cuenta que el nivel del riesgo no debe basarse únicamente en la clasificación de los Datos Personales (público, semiprivado, privado y sensible), en razón a que el impacto de un incidente de seguridad en los Datos Personales involucra un carácter contextual. Por ejemplo, el hurto de una base de datos que contiene los nombres de las personas junto con los números de identificación personal, la descripción de la finalidad o las fechas de nacimiento pueden representar un alto nivel de riesgo, mientras que, el hurto de una base de datos que contiene solo los nombres de las personas puede representar un riesgo menor.



Son factores que pueden ser tenidos en cuenta para determinar el nivel de riesgo:

En los Titulares de la información:

- ¿Qué cantidad de personas fueron afectadas?
- ¿Qué categoría de personas fueron afectadas?
- ¿Cuáles son las características especiales de las personas afectadas? Por ejemplo: niños, niñas y/o adolescentes; personas en estado de vulnerabilidad, etc.

En los datos personales:

- ¿Cuál fue el volumen de los datos afectados?
- ¿Cuál fue el periodo durante el cual los datos fueron afectados o estuvieron comprometidos?
- ¿Qué tipo de información personal fue afectada? Por ejemplo, identificación personal, datos biométricos, historia clínica, datos genéticos, pruebas académicas, registros de localización, direcciones IP, mensajes de texto, información financiera y crediticia, datos genéticos, perfiles de comportamiento, puntajes de crédito, etc.
- ¿Qué tan sensible es la información comprometida? Por ejemplo: datos de niños, niñas y/o adolescentes; datos biométricos, genéticos o de salud; perfiles de comportamiento; resultados de decisiones automatizadas; orientación sexual; datos políticos; etc.
- ¿Cuál es el contexto de la información personal comprometida?
- ¿Estaba la información personal adecuadamente cifrada, anonimizada? ¿Era inaccesible?
- ¿Cómo se puede utilizar la información personal afectada?
- ¿Existe un riesgo a una mayor exposición de la información personal?
- ¿Está la información personal disponible públicamente en internet?
- ¿Se puede utilizar la información personal para fines fraudulentos o puede causar cualquier tipo de daño material o inmaterial al Titular?
- ¿Se ha recuperado la información personal?

En la organización

- ¿Qué causó el incidente de seguridad?
- ¿Cuándo y con qué frecuencia ocurrió el incidente de seguridad?
- ¿Es este un problema sistémico o aislado?
- ¿Cuál fue el alcance del incidente de seguridad?
- ¿Qué medidas se han tomado para mitigar el daño?



- ¿Cuáles son las actividades y operaciones que desarrolla la organización? Por ejemplo: entidades financieras, entidades públicas, proveedores de aplicaciones móviles, colegios, farmacias, hospitales, almacenes de ropa, operadores de información, proveedores de redes sociales, etc.
- ¿Los datos comprometidos afectarán las transacciones que debe realizar la organización con terceros externos?

03. Identificar los daños para las personas, organizaciones y público en general

La identificación de los daños deberá abordar los siguientes interrogantes:

¿Qué daños para las personas podrían resultar de un incidente de seguridad?

Se deben identificar cualquiera de los siguientes daños:

- Riesgo en su seguridad física o psicológica
- Extorsión económica o sexual
- Hurto de identidad
- Suplantación de identidad
- Pérdida financiera
- Negación de un crédito o seguro
- Perfilamiento con fines ilícitos
- Pérdida de negocios u oportunidades de empleo
- Discriminación
- Humillación significativa o pérdida de dignidad y daño a la reputación.

¿Qué daño para la organización podría resultar de un incidente? Los ejemplos incluyen:

- Pérdida reputacional
- Pérdida de clientes o usuarios
- Pérdida de confianza en la organización
- Honorarios de consultores e ingenieros forenses
- Pérdida de activos
- Sanciones, órdenes e instrucciones administrativas
- Exposición financiera
- Órdenes judiciales
- Demandas judiciales

¿Qué daño para el público podría resultar de un incidente de seguridad? Los ejemplos incluyen:

- Riesgo para la salud pública
- Riesgo para la seguridad pública



- Pánico económico
- Alteración de los pilares constitucionales de un país

04. Notificar a la Superintendencia de Industria y Comercio

FUNDACIÓN SILARAA deberá reportar la ocurrencia del incidente de seguridad ante la SIC sin dilación indebida y a más tardar dentro los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos.

La notificación de un incidente de seguridad en Datos Personales debe contener, como mínimo, la información que establece el Registro Nacional de Bases de Datos (RNBD).

05. Comunicar a los Titulares de la información

Ocurrido el incidente de filtración, pérdida, publicación indebida de información, **FUNDACIÓN SILARAA** deberá informar de manera inmediata a todos los titulares de los datos personales que sufrieron dicho incidente. Si se tiene Backup o respaldo de la información, se deberá informar a través de los medios disponibles. En caso de que la pérdida de la base de datos suponga una pérdida total de la información de los titulares de los datos personales. Deberá emitirse avisos de carácter general, el cual se debe publicar en la página Web, redes sociales, carteleras entre otros. Para mitigar el riesgo de respaldo, se sugiere que cada base de datos se inscriba en el Registro Nacional de Bases de Datos.

La comunicación a los Titulares de la Información brinda la oportunidad para que ellos mismos puedan adoptar las medidas necesarias para protegerse de las consecuencias de un incidente de seguridad.

Las comunicaciones deben ser suficientes, claras y precisas para permitir que los Titulares de la información comprendan la importancia del incidente y que tomen las medidas, si es posible, para reducir los riesgos que podría resultar de su ocurrencia. Es primordial no incluir información personal innecesaria en el aviso para evitar una posible divulgación no autorizada.

06. Prevenir futuros incidentes de seguridad en Datos Personales

Una vez que se hayan tomado las medidas necesarias para mitigar los riesgos asociados con el incidente, **FUNDACIÓN SILARAA** deberá ejecutar un plan de prevención para evitar futuros eventos que puedan afectar los datos personales que han tratado.



Esto genera retos al interior de las organizaciones:

- Revisar las condiciones del Tratamiento.
- Realizar auditorías internas, externas o mixtas.
- Robustecer las políticas, procesos y procedimientos.
- Ajustar las evaluaciones de impacto en datos personales
- Establecer esquemas de trabajo a corto, mediano y largo plazo. Así como los roles y responsabilidades.
- Generar apoyo y compromiso de la Alta Gerencia para desplegar los cambios que se requieran al interior de las organizaciones.

Algunas de las medidas a implementar con posterioridad a la ocurrencia de un incidente pueden ser:

- Reforzar los programas de capacitación y educación del personal.
- Identificar y mejorar los controles internos que no tuvieron el efecto esperado en la contención de la brecha de seguridad.
- Identificar y eliminar malware o desactivar cuentas de usuarios vulnerables.
- Realizar un contraste con las medidas adoptadas para solucionar el incidente de seguridad en cuestión, y garantizar un análisis pormenorizado de las soluciones que pudieron haberse adoptado.
- Actualizar el antivirus.
- Analizar con el antivirus todo el sistema operativo, incluidas aquellas secciones que no se vieron afectadas.
- Garantizar que la estrategia adoptada encuentre un balance entre la continuidad del negocio y el riesgo intrínseco en los activos que se hayan visto afectados por el incidente de seguridad.
- Elaborar un informe final tendiente a recopilar la información, plazos de actuación y medidas adoptadas, de cara a una revisión por terceras personas.

19. REGISTRO NACIONAL DE BASES DE DATOS

FUNDACIÓN SILARAA se reserva, en los eventos contemplados en la ley y en sus estatutos y reglamentos internos, la facultad de mantener y catalogar determinada información que repose en sus bases o bancos de datos, como confidencial de acuerdo con las normas vigentes, sus estatutos y reglamentos.

FUNDACIÓN SILARAA, procederá de acuerdo con la normatividad vigente y la reglamentación que para tal fin expida el Gobierno Nacional, a realizar el registro de sus bases de datos, ante El Registro Nacional de Bases de Datos (RNBD) que será administrado por la Superintendencia de Industria y Comercio.



20. VIGENCIAS

La Presente Política de Privacidad regirá a partir del 01 Agosto de 2024.

Las bases de datos sujetas a tratamiento por parte del Responsable del tratamiento, estarán vigentes mientras subsistan las finalidades para las cuales se recolectaron los datos y/o el término que establezca la ley.

El Responsable del tratamiento se reserva el derecho de modificar en cualquier momento la presente Política de Privacidad. En caso de haber cambios sustanciales en el contenido de la misma, en relación con la identificación del Responsable del tratamiento y a la finalidad del tratamiento de los datos personales, los cuales puedan afectar el contenido de la autorización, el Responsable del tratamiento comunicará estos cambios al Titular antes de o a más tardar dentro de los diez (10) días hábiles siguientes al momento de implementar las nuevas políticas y requerirá una nueva autorización cuando el cambio se refiera a la finalidad del tratamiento.

21. TABLA DE SEGUIMIENTO Y CONTROL

Versión	Descripción	Fecha
1.0	Creación	01.08.2024

Firma

ROBERTO SÁNCHEZ ARBOUIN
Representante Legal
FUNDACIÓN SILARAA