1. OBJETIVO

Definir la Política de tratamiento y protección de datos personales para garantizar la protección de los derechos fundamentales de los titulares de los datos que administra DataSec SAS, como responsable del tratamiento de datos personales obtenidos en el marco de sus funciones comerciales y laborales como entidad de carácter privado, conforme a la ley 1581 de 2012 reglamentada parcialmente por el Decreto Nacional 1377 de 2013, reglamentada Parcialmente por el Decreto 1081 de 2015 y demás normas vigentes y complementarias que traten y regulen esta materia.

2. ALCANCE

Aplica a todos los datos personales cuyo titular sea una persona natural, administrados por DataSec SAS que requieren protección bajo los lineamientos de la Ley 1581 de 2012 y a todos los colaboradores, proveedores y contratistas que, en nombre de la compañía, debido a su labor, recolectan, almacenan, usan, circulan o supriman este tipo de datos.

3. IDENTIFICACIÓN DEL RESPONSABLE DEL TRATAMIENTO DE DATOS

Razón Social: DataSec SAS
NIT: 901.223.827-1
Dirección domicilio principal: Cra. 14A # 101-11 Oficina 201. Bogotá D.C.
Teléfono: 323 2901254
Correo electrónico: administrativo@datasec.com.co
Sitio web: www.datasasec.com.co

4. DEFINICIONES

- **Aviso de Privacidad:** Comunicación verbal o escrita generada por el responsable del tratamiento de datos personales, dirigida al titular de dichos datos, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de datos que le serán aplicables, la forma de acceder a estas y las finalidades del tratamiento que se pretende dar a los datos personales.
- **Autorización:** Consentimiento previo, expreso e informado del titular de los datos personales para llevar a cabo el tratamiento de dichos datos.
- **Bases de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento.
- **Dato Personal:** Cualquier información vinculada o que pueda asociarse a una o a varias personas naturales determinada. (persona individualmente considerada).
- **Dato personal público:** Toda información personal que es de conocimiento libre y abierto para el público en general.
- **Dato personal privado:** Es el que por su naturaleza íntima o reservada solo es relevante para el titular. Los gustos o preferencias de las personas, por ejemplo, corresponden a un dato privado.
- **Dato Público**: Es el que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales, y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- **Dato semiprivado:** Son los que no tienen naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo al titular sino a cierto sector o a la sociedad en general. Los datos financieros y crediticios de la actividad comercial o de servicios, son algunos ejemplos.
- **Dato Sensible**: Es el que afecta 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.
- **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.
- **Habeas Data:** Derecho de cualquier persona a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en el banco de datos y en archivos de entidades públicas y privadas.
- **Responsable del Tratamiento**: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.
- **Titular**: Persona natural cuyos datos personales sean objeto de tratamiento.

- **Transferencia:** Tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.
- **Transmisión:** Tratamiento de datos personales que implica la comunicación de estos 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.
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

5. PRINCIPIOS

Para lograr los objetivos de esta política se consideran los siguientes principios consagrados en la Ley 1581 de 2012:

- **Principio de legalidad en materia de tratamiento de datos:** El tratamiento a que se refiere la Ley 1582 de 2012 es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.
- **Principio de finalidad:** El tratamiento debe obedecer a una finalidad legítima de acuerdo con la constitución y la ley, lo cual debe ser informada al titular.
- **Principio de libertad:** El tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.
- **Principio de veracidad o calidad:** La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
- **Principio de transparencia:** En el tratamiento debe garantizarse el derecho del titular a obtener 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.
- **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 la presente ley y la Constitución. En este sentido, el tratamiento sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la Ley.
  Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la Ley.
- **Principio de seguridad:** La información sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento a que se refiere la Ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- **Principio de confidencialidad:** Todas las personas que intervengan en el tratamiento de datos personales 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 ello corresponda al desarrollo de las actividades autorizadas en la Ley.

6. TRATAMIENTO Y FINALIDADES A LAS CUALES SERÁN SOMETIDOS LOS DATOS

El tratamiento de los datos personales de empleados, clientes, proveedores, contratistas, o de cualquier persona con la cual DataSec SAS, establezca o estableciera una relación, permanente u ocasional, lo hará dentro del marco legal aplicable y serán los necesarios para el cumplimiento de la misión de la compañía.

De manera general, el tratamiento al que serán sometidos los datos personales de los titulares incluye la recolección, almacenamiento, uso, circulación y supresión.

En todo caso, los datos personales podrán ser recolectados y tratados para:

- Desarrollar la misión de la compañía conforme a su objeto social.
- Cumplir todos los compromisos contractuales.
- Cumplir las normas aplicables a proveedores y contratistas, incluyendo, pero sin limitarse a las tributarias y comerciales.
- Cumplir lo dispuesto por el ordenamiento jurídico colombiano en materia laboral y de seguridad social, seguridad y salud en el trabajo, entre otras, aplicables a exempleados, empleados actuales y candidatos a futuro empleo.
- Informar sobre oportunidades de empleo y/ o desarrollar los estudios previos y procesos de selección, contratación y vinculación a la compañía.

- Mantener actualizada la historia laboral y registros de nómina.
- Realizar el envío de información relacionada con programas, invitaciones, eventos, noticias, actividades, productos y demás bienes o servicios ofrecidos por DataSec SAS.
- Realizar encuestas relacionadas con los servicios o bienes de la compañía.
- Conservar evidencia de los eventos realizados para el desarrollo del objeto social.
- Registrar y/o autorizar el ingreso a las instalaciones de la compañía.
- Realizar monitoreo a través de sistemas de video vigilancia para mitigar riesgos de seguridad física y del entorno.
- Gestionar trámites, peticiones, quejas, reclamos, sugerencias y atender requerimientos de información de entes de control

Conservación y Temporalidad de los Datos: Los datos personales serán conservados únicamente durante el tiempo necesario para cumplir con la finalidad para la cual fueron recolectados, según lo aplicable al tema y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información o los datos involucrados. Una vez agotada dicha finalidad, los datos serán eliminados de las bases de datos de la compañía, salvo que exista una obligación legal o contractual que requiera su conservación por un período adicional.

7. DERECHOS DEL TITULAR DE LOS DATOS PERSONALES

A los titulares de los datos personales contenidos en las bases de datos de DataSec SAS, les asiste los siguientes derechos, contenidos en la Ley 1581 de 2012:

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 Ley 1581 de 2012.
c). Ser informado por DataSec o por el encargado del tratamiento respecto al tratamiento de su información, previa solicitud, respecto del uso que les ha dado a sus datos personales.
d). Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la 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 la Superintendencia de Industria y Comercio haya determinado que en el tratamiento el responsable o encargado han incurrido en conductas contrarias a esta ley y a la constitución.
f). Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

8. DEBERES DEL RESPONSABLE DEL TRATAMIENTO

Aviso de Privacidad.
La compañía informará a todos los titulares de los datos personales, en el momento de la recolección, acerca de la existencia de esta política de tratamiento de datos personales, el uso y la finalidad que se dará a los mismos, y los derechos que les asisten como titulares. El aviso de privacidad será presentado a través de medios físicos, electrónicos o verbales, de forma que garantice el acceso y conocimiento por parte del titular.

Autorización para el Tratamiento de Datos.
La compañía solicitará a los titulares de los datos personales su autorización previa, expresa e informada para el tratamiento de estos, indicando la finalidad del tratamiento, el uso que se dará a los datos y los derechos que les asisten. La autorización podrá otorgarse por escrito, verbalmente o mediante conductas inequívocas que permitan concluir de manera razonable que otorgó su consentimiento.

En virtud de lo dispuesto en el artículo 17 de la Ley 1581 de 2012, son otros deberes de DataSec SAS, para el tratamiento de los datos personales los siguientes:
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 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 Ley 1581 de 2012.
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 1581 de 2012.
k). Adoptar los procedimientos para garantizar el adecuado cumplimiento de la presente 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.
p). Cumplir la Ley, las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

9. DEBERES DEL ENCARGADO DEL TRATAMIENTO

Los Encargados del tratamiento deben cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la ley:

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 presente 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 políticas y procedimientos para garantizar el adecuado cumplimiento de la 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 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.

10. ENCARGADOS DEL TRATAMIENTO

Los encargados del tratamiento de datos de los clientes son: Gerente Comercial, Gerente de Cuenta, Gestor Comercial y los cargos de las Áreas Financiera, Operativa y PMO autorizados a manejar datos con el propósito de prestar los servicios y cumplir el objeto social de la compañía.

Los encargados del tratamiento de datos de los proveedores son: Coordinador Administrativo, responsable de compras y Gerente Financiero y Administrativo.

Los encargados del tratamiento de datos de los empleados es el Director de Talento Humano.

El personal del área T.I, también son encargados del tratamiento de datos, ya que son administradores de las herramientas tecnológicas donde se almacenan los datos personales de las partes interesadas.

11. PROCEDIMIENTO PARA LA ATENCIÓN DE CONSULTAS, RECLAMOS, PETICIONES DE RECTIFICACIÓN, ACTUALIZACIÓN Y SUPRESIÓN DE DATOS.

a. Consultas:

Los titulares podrán consultar sus datos personales almacenados por DataSec SAS, quien garantiza medios de comunicación pertinentes, para atender las solicitudes de consulta 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 10 días, 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. Las consultas podrán formularse al correo: administrativo@datasec.com.co.

El Titular que considere que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la ley, podrán presentar un reclamo ante DataSec SAS, el cual será tramitado así:

1. Formular solicitud al correo administrativo@datasec.com.co, con la identificación del titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y los documentos aplicables.

Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que complete la información. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo. En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

2. Una vez recibido el reclamo completo, éste se catalogará con la etiqueta «reclamo en trámite» y el motivo de este, en un término no mayor a dos (2) días hábiles. Dicha etiqueta se mantendrá hasta que el reclamo sea decidido.

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

c. Petición de actualización y/o rectificación:

DataSec SAS rectificará y actualizará, a solicitud del titular, la información de éste que resulte incompleta o inexacta, de conformidad con el procedimiento y los términos antes señalados, para lo cual:

1. El titular deberá allegar la solicitud al correo administrativo@datasec.com.co indicando la actualización y/o rectificación a realizar y aportará la documentación que sustente su petición.

2. DataSec SAS podrá habilitar mecanismos que le faciliten el ejercicio de este derecho al titular, siempre y cuando éstos lo beneficien. En consecuencia, se podrán habilitar medios electrónicos u otros que considere pertinentes, los cuales serán informados se pondrán a disposición de los interesados en la página web.

d. Petición de supresión de datos:

El titular de los datos personales tiene el derecho de solicitar a DataSec SAS la supresión (eliminación) en cualquiera de los siguientes eventos:

1. Considere que los mismos no están siendo tratados conforme a los principios, deberes y obligaciones previstas en la normatividad vigente.

2. Hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recabados.

3. Se haya superado el periodo necesario para el cumplimiento de los fines para los que fueron recabados.

Esta supresión implica la eliminación total o parcial de la información personal de acuerdo con lo solicitado por el titular en los registros, archivos, bases de datos o tratamientos realizados por DataSec SAS. Sin embargo, este derecho del titular no es absoluto y en consecuencia DataSec SAS, podrá negar el ejercicio de este cuando:

a). El titular tenga un deber legal o contractual de permanecer en la base de datos.

b). La eliminación de datos obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas.

c). Los datos sean necesarios para proteger los intereses jurídicamente tutelados del titular; para realizar una acción en función del interés público, o para cumplir con una obligación legalmente adquirida por el titular.

12. MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN.

Dando cumplimiento al principio de seguridad establecido en la normatividad vigente, DataSec SAS, adopta las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los datos personales evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Entre otras, a continuación, se indican algunas de las medidas tomadas por la organización:

- Las políticas de seguridad se actualizan para que permanezcan alineadas con las tecnologías de seguridad y control utilizadas.
- Se definen políticas y controles para hacer un uso aceptable de los activos, asegurar las redes y la transferencia de la información.
- Los líderes de proceso, colaboradores y terceros a nombre de DataSec SAS, velan por el cumplimiento de las políticas de seguridad de la información, la protección de los activos de información y los datos personales que administran.
- El acceso lógico y físico a los sistemas, la información y a los datos personales, por parte de los colaboradores y terceros, se controla de acuerdo con el rol que vayan a desempeñar, funciones y autorizaciones desde el Proceso de T.I. a través del directorio activo, previa aprobación del Líder del proceso, y se otorga de acuerdo con los controles y privilegios de acceso definidos.
- Cualquier actividad realizada por un colaborador o tercero en los sistemas de información del SOC, es monitoreada. En el caso que se identifiquen riesgos de seguridad sobre la información, inmediatamente será revocada su autorización y el sistema será bloqueado.
- Se realiza la inactivación del usuario, al momento de finalizar el contrato o al concluir con las actividades requeridas y todo acceso a los sistemas de información otorgado a colaboradores, proveedores o entes de control.
- Se definen lineamientos para la configuración de contraseñas que aplican sobre las plataformas tecnológicas, los servicios de red y los sistemas de información; dichos lineamientos consideran aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, la no visualización en la introducción de contraseñas, usuarios individuales para cada colaborador, entre otros.
- Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. En consecuencia, cuentan con medidas de control de acceso físico en el perímetro, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.
- Las instalaciones de procesamiento de la información se encuentran físicamente protegidas adecuadamente contra acceso no autorizado; las puertas permanecen cerradas cuando no hay supervisión del personal autorizado para ingresar a las mismas. Adicionalmente, se cuenta con un sistema CCTV para dejar registro de las personas que ingresan y se retiran de estas áreas.
- El líder del proceso y demás colaboradores responsables de la gestión de información, deben garantizar que la información clasificada como reservada o restringida, sea cifrada al momento de almacenarse y/o transmitirse por cualquier medio.
- Se asegura la realización de copias de respaldo de los activos de información críticos, según lo establecido en el procedimiento de Copias de respaldo.
- Se asegura que las copias de respaldo generadas sean cifradas antes de guardarse, evitando fuga de información o pérdida de integridad.
- Se realizan pruebas de restauración de las copias de respaldo a la información de las estaciones de trabajo, permitiendo dejar evidencia documentada de las pruebas realizadas.
- Para la reasignación o disposición final de un equipo, se implementan métodos de borrado seguro de la información.
- El software instalado está aprobado por el área de Tecnología, cumpliendo con las disposiciones legales.
- Se cuenta con aplicaciones y herramientas tecnológicas que permiten controlar las posibles amenazas a los activos de información de DataSec SAS y detectar y remediar posibles vulnerabilidades.
- Las conexiones remotas, como VPN y Escritorios remotos, están controladas para que sean seguras.
- El acceso a equipos, servicios y aplicativos cuenta con métodos de autenticación que evitan accesos no autorizados.
- Los eventos e incidentes de seguridad de la información son reportados y gestionados al interior de la compañía para proteger los activos de la información, según lo definido en el Procedimiento para la Gestión de eventos e incidentes de seguridad de información, que describe las actividades de detección, identificación, reporte, evaluación, investigación, tratamiento y aprendizaje de los incidentes de la seguridad de la información que se puedan presentar, teniendo en cuenta el nivel de criticidad del ataque y de los activos, con el fin de garantizar la solución oportuna y eficaz.
- La compañía cuenta con un proceso SOC (Centro de Operaciones de Seguridad, que trabaja por la prevención de incidentes de Seguridad de la información, a través de la vigilancia constante de nuevas amenazas e implementación de controles preventivos que mitiguen el riesgo de aparición de incidentes de seguridad.
- Se identifican las debilidades a través de auditorías periódicas dirigidas a diferentes puntos de la infraestructura tecnológica para identificar debilidades, determinar las acciones correctivas y eliminar las vulnerabilidades.

- Se realiza monitorización continúa de la seguridad de la información, observando constantemente todos los controles de seguridad implementados con el objetivo de detectar posibles incidentes de seguridad. Para lograrlo el SOC se apoya en diferentes herramientas que le proporcionan información completa y en tiempo real del estado en que se encuentra la seguridad de DataSec.

13. VIGENCIA

La presente Política para el Tratamiento de Datos Personales rige a partir del **1 de septiembre de 2025.** Las bases de datos en las que se registrarán los datos personales tendrán una vigencia igual al tiempo en que se mantenga y utilice la información para las finalidades descritas en esta política. Una vez se cumpla(n) esa(s) finalidad(es) y siempre que no exista un deber legal o contractual de conservar la información, los datos serán eliminados de nuestras bases de datos.

Se registran actualizaciones de acuerdo con el siguiente control de cambios:

14. CONTROL DE CAMBIOS

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	25/07/2023	Creación del documento
2	18/01/2024	Se actualiza dirección de la nueva oficina de la compañía. Numeral 10 se actualizan algunos cargos de encargados de tratamiento de datos.
3	01/09/2025	Revisión anual de la idoneidad, vigencia y actualización de la Política.