MODIFICACIONES

FECHA	PÁGINA MODIFICADA	MODIFICACIÓN Nro.	CONTENIDO DE LA MODIFICACIÓN
26 septiembre de 2013	3	1	Derechos del titular
27 de julio de 2018	6	2	Procedimientos para conocimiento, recolección, actualización, supresión revocación y rectificación
3 de febrero de 2022	4, 6	3	Cambio de dirección de oficina
6 de febrero de 2023	Todo el documento	4	Inclusión de numerales y modificación de directrices
5 de febrero de 2025	2, 18	5	Cambios en correos
FECHA PRIMERA EDICIÓN: 26 de septiembre de 2013		PUESTA AL DÍA: 5 de febrero de 2025	

POLÍTICAS Y MANUAL DE TRATAMIENTO DE DATOS PERSONALES

NGS&O ABOGADOS S.A.S., en cumplimiento de la normativa vigente, adopta la presente política para el tratamiento de datos personales, la cual será informada a todos los titulares de los datos recolectados o que en el futuro se obtengan en el ejercicio de sus actividades. De esta manera, manifestamos que garantizamos los derechos de la privacidad y la intimidad, en el tratamiento de los datos personales y, en consecuencia, todas sus actuaciones se regirán por los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad. Todas las personas que, en desarrollo de diferentes actividades, sean permanentes u ocasionales, llegaren a suministrar cualquier tipo de información o dato personal, podrá conocerla, actualizarla y rectificarla. La presente política será aplicable a los datos personales registrados en cualquier base de datos, cuyo titular sea una persona natural.

Capítulo I

Políticas y Seguridad de Procedimientos

1. Base legal y ámbito de aplicación.

El derecho a la Protección de los Datos tiene como finalidad permitir a todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en archivos o bases de datos.

Cuando el Titular de los datos presta su consentimiento para que estos formen parte de una base de datos de una institución, pública o privada, jurídica o natural, ésta se hace mediante el responsable del tratamiento de estos datos y adquiere una serie de obligaciones como son: la de tratar dichos datos con seguridad y cautela, velar por su integridad y aparecer como órgano a quien el Titular puede dirigirse para el seguimiento de la información y el control de la misma, pudiendo ejercitar los derechos de consultas y reclamos.

Si bien, la responsabilidad del tratamiento de los datos recae en el responsable del tratamiento, sus competencias se materializan en las funciones que corresponden a su personal de servicio. El personal de la institución responsable del tratamiento con acceso, directo o indirecto a las bases de datos que contienen los datos personales debe conocer la normativa de protección de datos, la política de protección de datos de la

organización; y deben cumplir con las obligaciones en materia de seguridad de los datos correspondientes a sus funciones y cargo.

Para velar con el cumplimiento de sus obligaciones de seguridad, los responsables del tratamiento nombran a su **representante legal** como encargado de desarrollar, coordinar, controlar y verificar el cumplimiento de las medidas de seguridad recogidas en este manual.

Esta política será aplicable a todos los datos personales registrados en bases de datos que sean objeto de tratamiento por el responsable del tratamiento y se encuentra dirigida a todos los usuarios de datos, que son tanto el personal propio como al personal externo del responsable del tratamiento.

Todos los usuarios identificados en el presente documento de Seguridad están obligados a cumplir con las medidas de seguridad establecidas para el tratamiento de los datos y están sujetos al deber de confidencialidad, incluso después de acabada su relación laboral o profesional con la organización responsable del tratamiento. El deber de confidencialidad, se formaliza a través de la firma de un acuerdo de confidencialidad, suscrito entre el usuario y el responsable del tratamiento.

2. Definiciones.

- **Acceso autorizado**: Autorización concedida a un usuario para el uso de determinados recursos. En dispositivos automatizados es el resultado de una autentificación correcta, generalmente mediante el ingreso de usuario y contraseña.
- **Autenticación:** Procedimiento de verificación de la identidad de un usuario.
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.
- **Aviso de privacidad:** Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.
- **Base de Datos:** Conjunto organizado de datos personales que sea objeto de tratamiento.
- **Contraseña**: Seña secreta que permite el acceso a dispositivos, información o bases de datos antes inaccesibles. Se utiliza en la autentificación de usuarios que permite el acceso autorizado.

- **Control de acceso**: Mecanismo que permite acceder a dispositivos, información o bases de datos mediante la autentificación.
- **Copia de respaldo**: Copia de los datos de una base de datos en un soporte que permita su recuperación.
- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Dato público:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- **Datos sensibles:** Se entiende por datos sensible 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.
- **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.
- **Identificación**: Proceso de reconocimiento de la identidad de los usuarios.
- **Incidencia**: Cualquier anomalía que afecte o pueda afectar a la seguridad de los datos, constituyendo un riesgo para la confidencialidad, disponibilidad o integridad de las bases de datos o de los datos personales que contienen.
- **Perfil de usuario**: Grupo de usuarios a los que se da acceso.
- **Recurso protegido**: Cualquier componente del sistema de información, como bases de datos, programas, soportes o equipos, empleados para el almacenamiento y tratamiento de datos personales.
- **Responsable de seguridad**: Una o varias personas designadas por el responsable del tratamiento para el control y la coordinación de las medidas de seguridad.
- **Sistema de información**: Conjunto de bases de datos, programas, soportes y/o equipos empleados para el tratamiento de datos personales.
- **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.

- **Soporte**: Material en cuya superficie se registra información o sobre el cual se pueden guardar o recuperar datos, como el papel, la cinta de video, el CD, el DVD, el disco duro, etc.
- **Usuario**: Sujeto autorizado para acceder a los datos o recursos, o proceso que accede a los datos o recursos sin identificación de un sujeto.
- **Titular:** Persona natural cuyos datos personales sean objeto de tratamiento.
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- **Transferencia:** La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.
- **Transmisión:** Tratamiento de datos personales que implica la comunicación de 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.

3. Principios de la protección de datos.

Existen unos principios para el tratamiento de datos personales que se han de aplicar, de manera armónica e integral, en el desarrollo, interpretación y aplicación de la Ley. Los principios legales de la protección de datos son los siguientes:

Principio de legalidad.

Principio de finalidad: El tratamiento debe obedecer a una finalidad legítima, la cual debe ser informada al Titular.

Principio de libertad: El tratamiento solo 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 revele el consentimiento. El tratamiento de los datos requiere la autorización previa e informada del Titular por cualquier medio que permita ser consultado con posterioridad, salvo en los siguientes casos:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.

- Tratamiento de información autorizado por la Ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las personas.

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. En el momento de solicitar la autorización al titular, el responsable del tratamiento deberá informarle de manera clara y expresa lo siguiente, conservando prueba del cumplimiento de este deber:

- El tratamiento al cual será sometidos sus datos y la finalidad del mismo.
- El carácter facultativo de la respuesta del Titular a las preguntas que le sean hechas cuando éstas traten sobre datos sensibles o sobre datos de niños, niñas o adolescentes.
- Los derechos que le asisten como Titular.
- La identificación, dirección física, el correo electrónico y el teléfono del responsable del tratamiento.

Principio de acceso y circulación restringida: El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales. En este sentido, el tratamiento solo 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 y otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo 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 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. El responsable del tratamiento tiene la responsabilidad de implantar las medidas de seguridad correspondientes y de ponerlas en conocimiento todo personal que tenga acceso, directo o indirecto, a los datos. Los

usuarios que accedan a los sistemas de información del responsable del tratamiento deben conocer y cumplir con las normas y medidas de seguridad que correspondan a sus funciones. Estas normas y medidas de seguridad se recogen en el presente documento, de obligatorio cumplimiento para todo usuario y personal del responsable del tratamiento; cualquier modificación de las normas y medidas en materia de seguridad de datos personales por parte del responsable del tratamiento ha de ser puesta en conocimiento de los usuarios.

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 solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas.

4. Categorías especiales de datos.

4.1. Datos sensibles.

Los 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.

Se prohíbe el tratamiento de datos sensibles, excepto cuando:

- El Titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.
- El tratamiento sea necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
- El tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular.

- El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- El tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

4.2. Derechos de los niños, niñas y adolescentes

El tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, y cuando dicho tratamiento cumpla con los siguientes requisitos:

- Que responda y respete el interés superior de los niños, niñas y adolescentes.
- 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 a su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás.

Todo responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos, cumpliendo en todo momento con los principios y obligaciones. En todo caso, el tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.

Los derechos de acceso, corrección, supresión, revocación o reclamo por infracción sobre los datos de los niños, niñas adolescentes se ejercerán por las personas que estén facultadas para representarlos.

4.3 Derechos de los Titulares.

Los Titulares de los datos pueden ejercer una serie de derechos en relación con el tratamiento de sus datos personales. Estos derechos podrán ejercerse por las siguientes personas.

- Por el Titular, quién deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.
- Por sus causahabientes, quienes deberán acreditar tal calidad.
- Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.
- Por estipulación a favor de otro y para otro.

Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

Los derechos del Titular son los siguientes:

- **Derecho de acceso o consulta:** Se trata del derecho del Titular a ser informado por el responsable del tratamiento, previa solicitud, respecto al origen, uso y finalidad que les han dado a sus datos personales.
- **Derechos de quejas y reclamos**. La Ley distingue cuatro tipos de reclamos:
    - **Reclamo de corrección:** el derecho del Titular a que se actualicen, rectifique o modifiquen aquellos datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
    - **Reclamo de supresión:** el derecho del Titular a que se supriman los datos que resulten inadecuados, excesivos o que no respeten los principios, derechos y garantías constitucionales y legales.
    - **Reclamo de revocación:** el derecho del Titular a dejar sin efecto la autorizaciónpreviamente prestada para el tratamiento de sus datos personales.
    - **Reclamo de infracción:** el derecho del Titular a solicitar que se subsane el incumplimiento de la normativa en materia de Protección de Datos.

- **Derecho a solicitar prueba de la autorización otorgada al responsable del tratamiento.**
- **Derecho a presentar ante las Autoridades Locales quejas por infracciones:** el Titular o causahabiente solo podrá elevar esta queja una vez haya agotado el trámite de consulta o reclamo ante el responsable del tratamiento o encargado del tratamiento.

- **Derecho a Abstenerse de responder las preguntas sobre datos sensibles**. Tendrá carácter facultativo las respuestas que versen sobre datos sensibles o sobre datos de los menores de edad.

5. Autorización de la política de tratamiento.

Para el tratamiento de datos personales, se requiere la autorización previa e informada del Titular. Mediante la aceptación de la presente política, todo Titular que facilite información relativa a sus datos personales está consintiendo el tratamiento de sus datos por parte del responsable del tratamiento, en los términos y condiciones recogidos en la misma.

No será necesaria la autorización del Titular cuando se trate de:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las personas.

Menores de edad:

Los datos personales de los **menores de edad** tienen una especial protección y por lo tanto su tratamiento está prohibido, excepto cuando se trate de datos de naturaleza pública, y cuando dicho tratamiento cumpla con los siguientes parámetros y requisitos:

- Que responda y respete el interés superior de los niños, niñas y adolescentes.
- 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. Todo responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos.

6. Responsable del tratamiento.

El responsable del tratamiento de las bases de datos, objeto de esta política, es NGS&O ABOGADOS S.A.S.

NIT: 900.151.350-5

DIRECCIÓN: Calle 100 8 A – 55, oficina 309, de Bogotá.

MAIL: asistenteadministrativo@ngsoabogados.com

TELÉFONO: 601 4320170

6.1. Las obligaciones del responsable del tratamiento.

Las obligaciones en materia de seguridad de los datos personales tratados por el responsable del tratamiento son las siguientes:

- Coordinar e implantar las medidas de seguridad recogidas en el presente documento.
- Difundir el referido documento entre el personal afectado.
- Mantener este Manual actualizado y revisado siempre que se produzcan cambios relevantes en el sistema de información, el sistema de tratamiento, la organización de la institución, el contenido de la información de las bases de datos, o como consecuencia de los controles periódicos realizados. De igual modo, se revisará su contenido cuando se produzca algún cambio que pueda afectar al cumplimiento de las medidas de seguridad.
- Designar uno o más responsables de seguridad e identificar a los usuarios autorizados para acceder a las bases de datos.
- Cuidar que el acceso mediante sistemas y aplicaciones informáticas se lleve a cabo mediante acceso identificado y contraseña.
- Autorizar, salvo delegación expresa a usuarios autorizados e identificados en este Manual, la salida de soportes fuera de los establecimientos donde se encuentran las bases de datos; las entradas y salidas de información por red, mediante dispositivos de almacenamiento electrónico o en papel y el uso de módems y las descargas de datos.
- Verificar la correcta aplicación del procedimiento de copias de respaldo y recuperación de datos.
- Garantizar la existencia de una lista de usuarios autorizados y perfiles de usuario.

- Analizar periódicamente, junto con el responsable de seguridad correspondiente, las incidencias registradas para establecer las medidas correctoras oportunas.
- Realizar verificaciones internas para garantizar el cumplimiento de las medidas de seguridad en materia de protección de datos.

6.2. Deberes de NGS&O ABOGADOS S.A.S. como responsable del tratamiento de los datos personales:

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

b. Solicitar y conservar, copia de la respectiva autorización otorgada por el titular para el tratamiento de datos personales.

c. Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten en 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 sea veraz, completa, exacta, actualizada, comprobable y comprensible.

f. Actualizar oportunamente la información, atendiendo de esta forma todas las novedades respecto de los datos del titular. Adicionalmente, se deberán implementar todas las medidas necesarias para que la información se mantenga actualizada.

g. Rectificar la información cuando sea incorrecta y comunicar lo pertinente.

h. Respetar las condiciones de seguridad y privacidad de la información del titular.

i. Tramitar las consultas y reclamos formulados en los términos señalados por la ley.

j. Identificar cuando determinada información se encuentra en discusión por parte del titular.

k. Informar a solicitud del titular sobre el uso dado a sus datos.

l. 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.

m. Cumplir los requerimientos e instrucciones que imparta la Superintendencia de Industria y Comercio sobre el tema en particular.

n. Usar únicamente datos cuyo tratamiento esté previamente autorizado.

o. Velar por el uso adecuado de los datos personales de los niños, niñas y adolescentes, en aquellos casos en que se entra autorizado el tratamiento de sus datos.

p. Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la ley.

q. 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.

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

s. Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.

t. Usar los datos personales del titular sólo para aquellas finalidades para las que se encuentre facultada debidamente y respetando en todo caso la normatividad vigente sobre protección de datos personales.

6.2. Cámaras de seguridad y filmación dentro de las instalaciones de la entidad

Los datos capturados por nuestras cámaras de seguridad y sistemas de control de acceso a funcionarios, clientes corporativos, clientes de servicio, visitantes o público en general, serán tratados con fines de seguridad, controlados por un sistema independiente de monitoreo y supervisión acorde a la prestación de seguridad de la compañía, sus instalaciones o funcionarios. Los datos tratados por estos sistemas son custodiados únicamente por NGS&O ABOGADOS S.A.S., y en caso de asignarse un encargado debe brindar las condiciones de seguridad, confidencialidad y demás requerimientos de las presentes políticas de datos personales.

7. Tratamiento y finalidades de las bases de datos

NGS&O ABOGADOS S.A.S., en el desarrollo de sus actividades, lleva a cabo el tratamiento de datos personales relativos a personas naturales que están contenidos y son tratados en bases de datos destinadas a finalidades legítimas.

NGS&O ABOGADOS S.A.S. podrá recolectar datos personales, a través de los distintos medios (físicos o digitales). En todo caso, la recolección se hará bajo expresa autorización del titular de los datos y el tratamiento de estos, estará sujeto a lo establecido por la ley.

De acuerdo con las autorizaciones impartidas por los titulares de la información, NGS&O ABOGADOS S.A.S. realizará operaciones o conjunto de operaciones que incluyen recolección de datos, su almacenamiento, uso, circulación y/o supresión, entrega de los datos a terceras entidades a título de encargados o de responsables; esto de acuerdo con el acuerdo al que entre las partes se llegue. Este Tratamiento de datos se realizará exclusivamente para las finalidades autorizadas y previstas en la presente Política y en las autorizaciones específicas otorgadas por parte del titular. De la misma forma se realizará Tratamiento de Datos Personales cuando exista una obligación legal o contractual para ello, siempre bajo los lineamientos de las políticas de Seguridad de la Información del responsable del tratamiento, en todos los casos los datos personales podrán ser tratados con la finalidad de adelantar los procesos de control y auditorías internas y externas y evaluaciones que realicen los organismos de control. Así mismo y en ejecución del objeto social de las sociedades que componen NGS&O ABOGADOS S.A.S., los datos personales serán tratados de acuerdo con el grupo de interés y en proporción a la finalidad o finalidades que tenga cada tratamiento, como se describe a continuación:

La siguiente tabla presenta las distintas **bases de datos** y las **finalidades** asignadas a cada una de ellas:

Tabla I.

Bases de datos y finalidades

EMPLEADOS, PRACTICANTES, CANDIDATOS A VACANTES:

1. Administrar y operar, directamente o por conducto de terceros, los procesos de selección y vinculación de personal, incluyendo la evaluación y calificación de los

participantes y la verificación de referencias laborales y personales, la realización de estudios de seguridad y de antecedentes;
2. Desarrollar las actividades propias de la gestión de recursos humanos, tales como nómina, afiliaciones a entidades del sistema general de seguridad social, actividades de bienestar y salud ocupacional, ejercicio de la potestad sancionatoria del empleador, entre otras;
3. Realizar los pagos necesarios derivados de la ejecución del contrato de trabajo y/o su terminación, y las demás prestaciones sociales a que haya lugar de conformidad con la ley aplicable;
4. Enviar todo tipo de comunicaciones relacionadas con las actividades propias de recursos humanos y de la administración del personal humano;
5. Contratar beneficios laborales con terceros, tales como seguros de vida, gastos médicos, entre otros;
6. Notificar a contactos autorizados en caso de emergencias durante el horario de trabajo o con ocasión del desarrollo del mismo;
7. Coordinar el desarrollo profesional de los empleados, el acceso de los empleados a los recursos informáticos del Empleador y asistir en su utilización;
8. Planificar actividades empresariales;
9. Controlar el acceso a las oficinas y establecer medidas de seguridad;
10. Transferir y/o transmitir la información recolectada a favor de sus compañías vinculadas en Colombia y en el exterior, y a encargados y/o responsables nacionales y extranjeros, a terceros, cuando ello sea necesario para el desarrollo de sus operaciones y gestión de nómina (recaudo de cartera y cobros administrativo, tesorería, contabilidad, entre otros);
11. Capacitar a su personal y enviarle comunicaciones de todo tipo.
12. Utilizar los datos privados y semiprivados para las finalidades acá mencionadas. Los datos sensibles se utilizarán para videovigilancia y seguridad.
13. Cualquier otra actividad de naturaleza similar a las anteriormente descritas que sean necesarias para desarrollar el objeto social.

PROVEEDORES DE BIENES Y SERVICIOS

1. Recolectar, registrar, actualizar y mantener sus datos personales con la finalidad de informar, comunicar, organizar, controlar, atender, acreditar las actividades en relación a su condición de proveedor y personal contratista de la sociedad
2. Analizar aspectos financieros, técnicos y de cualquier otro tipo que permita a la sociedad, identificar la capacidad de cumplimiento del proveedor.
3. Desarrollar y aplicar procesos de selección, evaluación, elaboración de respuestas a una solicitud de información, elaborar solicitudes de cotización y propuesta, y/o adjudicación de contratos.

4. Administrar los datos de carácter personal para realizar pagos a proveedores, incluida la administración de los números de cuentas bancarias para la correcta gestión de los pagos a realizar por parte de la sociedad
5. Gestionar los datos del PROVEEDOR para efectuar los procesos de pagos de facturas y cuentas de cobro presentadas a la sociedad.
6. Cumplir las obligaciones derivadas de la relación comercial que se establezca con EL PROVEEDOR.
7. Exigir el cumplimiento de las obligaciones a cargo del PROVEEDOR.
8. Asignar controles físicos y lógicos a las instalaciones y activos informáticos y de información propiedad de la sociedad.
9. Administrar y operar, directamente o por conducto de terceros, los procesos de selección y vinculación de PROVEEDORES, incluyendo la evaluación y calificación de los proveedores y la verificación de referencias laborales y personales, la realización de estudios de seguridad y de antecedentes;
10. Desarrollar las actividades propias de la gestión de recursos humanos dentro de la Compañía, tales como afiliaciones a entidades del sistema general de seguridad social y similares;
11. Realizar los pagos necesarios derivados de la ejecución del contrato de servicios y/o su terminación;
12. Enviar todo tipo de comunicaciones relacionadas con la relación precontractual y contractual con el proveedor;
13. Notificar a contactos autorizados en caso de emergencias en desarrollo de los servicios del proveedor;
14. Planificar actividades empresariales;
15. Controlar el acceso a las oficinas de la Compañía y establecer medidas de seguridad;
16. Transferir y/o transmitir la información recolectada a favor de sus compañías vinculadas en Colombia y en el exterior, y a encargados y/o responsables nacionales y extranjeros, a terceros, cuando ello sea necesario para el desarrollo de sus operaciones (recaudo de cartera y cobros administrativo, tesorería, contabilidad, entre otros);
17. Registrar a los contratistas y proveedores en los sistemas de la Compañía y procesar sus pagos;
18. Capacitar a los proveedores en políticas de la Compañía;
19. Utilizar los datos privados y semiprivados para las finalidades acá mencionadas. Los datos sensibles se utilizarán para videovigilancia y seguridad.
20. Cualquier otra actividad de naturaleza similar a las anteriormente descritas que sean necesarias para desarrollar el objeto social de la Compañía.

CLIENTES Y CLIENTES POTENCIALES

1. Enviar información sobre cambios en las condiciones de los servicios y productos ofrecidos por la sociedad;
2. Brindar seguridad personal.
3. Enviar información sobre ofertas relacionadas con los servicios y productos que ofrece la sociedad y sus compañías vinculadas;
4. Captar información personal a través de medios electrónicos, tales como páginas web y portales de redes sociales, a efectos de enviar al cliente publicidad de los servicios de la Compañía y de terceros relacionados con el mismo sector.
5. Facilitar el diseño e implementación de programas de fidelización;
6. Llevar a cabo procesos de auditoría interna o externa propios de la actividad comercial que la sociedad desarrolla;
7. Controlar el acceso a las instalaciones de la Compañía y establecer medidas de seguridad, incluyendo el establecimiento de zonas video-vigiladas;
8. Dar respuesta a consultas, peticiones, quejas y reclamos que sean realizadas por los Titulares y a organismos de control y demás autoridades que en virtud de la ley aplicable deban recibir los Datos Personales;
9. Transferir y/o transmitir la información recolectada a favor de sus compañías vinculadas en Colombia y en el exterior, y a encargados y/o responsables nacionales y extranjeros, a terceros, cuando ello sea necesario para el desarrollo de sus operaciones (recaudo de cartera y cobros administrativo, tesorería, contabilidad, marketing, entre otros);
10. Utilizar los distintos servicios correspondientes a sitios web, incluyendo descargas de contenidos y formatos;
11. Registrar sus datos personales en los sistemas de información de la sociedad y en sus bases de datos comerciales y operativas;
12. Utilizar los datos privados y semiprivados para las finalidades acá mencionadas. Los datos sensibles se utilizarán para videovigilancia y seguridad.
13. Cualquier otra actividad de naturaleza similar a las anteriormente descritas que sean necesarias para desarrollar el objeto social de la Compañía.

ACCIONISTAS Y ADMINISTRADORES DE LA SOCIEDAD

Los datos personales de los accionistas y miembros de Junta Directiva de la sociedad, se encuentran registrados en los libros de accionistas de la compañía y archivo o carpeta física y/o digital. Este tipo de información tiene por mandato legal el carácter de reservada. El tratamiento de datos personales de accionistas y miembros de Junta Directiva de la sociedad, se llevará a cabo conforme a lo establecido en el Código de Comercio y demás normas análogas o que regulen esta materia. Las finalidades que se

aplicarán a los datos personales de los accionistas y miembros de Junta Directiva serán las siguientes:

1. Verificación de antecedentes.
2. Enviar comunicaciones y convocatorias sobre asuntos de la sociedad, reuniones de asamblea y junta directiva.
3. Tramitar pagos de honorarios y similares.
4. Realizar reportes a entes de control y autoridades públicas.
5. Garantizar los deberes y derechos que se deriven de la calidad de accionistas y miembros de Junta Directiva.
6. Recolectar, registrar y actualizar los datos personales de accionistas y miembros de Junta Directiva con la finalidad de informar las actividades que lleva a cabo la sociedad, en relación a su condición de accionista y miembro de Junta Directiva.
7. Utilizar los datos privados y semiprivados para las finalidades acá mencionadas, hasta donde la ley lo permita.
8. Cualquier otra actividad de naturaleza similar a las anteriormente descritas que sean necesarias para desarrollar el objeto social de la Compañía.

7. 1 Atención a los Titulares de datos

Cada cliente tiene derecho a obtener información y a acceder a sus datos personales recogidos, con sujeción a las disposiciones legales aplicables. También le asisten los derechos de rectificación, supresión y limitación del tratamiento de sus datos. Además, el cliente tiene derecho a la portabilidad de los datos y a definir instrucciones para su tratamiento después de su fallecimiento. Puede incluso oponerse al tratamiento de sus datos.

Si desea ejercer alguno de estos derechos, póngase en contacto directamente con ***"NGS&O ABOGADOS S.A.S."****, a través del correo electrónico en la dirección* ***asistenteadministrativo@ngsoabogados.com***

Con el fin de garantizar la confidencialidad y la protección de sus datos personales, deberemos identificarlo para responder a su solicitud. Para ello, si existe alguna duda razonable sobre su identidad, le pediremos que adjunte como apoyo para su solicitud una copia de un documento oficial de identidad.

Todas las solicitudes se procesarán con la mayor brevedad posible y de conformidad con la legislación aplicable.

Encontrará toda la información necesaria para ponerse en contacto con NGS&O ABOGADOS S.A.S. en el sitio web ***www.ngsoabogados.com****. Para obtener asistencia durante estos procesos, escriba al buzón* ***asistenteadministrativo@ngsoabogados.com***

8. Procedimientos para ejercer los derechos del Titular.

8.1. Derecho de acceso o consulta.

El Titular de los datos puede ejercitar el derecho de acceso o consulta de sus datos mediante un escrito dirigido al correo electrónico ***asistenteadministrativo@ngsoabogados.com***, indicando en el asunto "ejercicio del derecho de acceso o consulta" la solicitud deberá contener los siguientes datos:

- Nombres y apellidos del Titular y/o su representante y/o causahabientes;
- Lo que se pretende consultar
- Documentos acreditativos de la petición formulada que se quieran hacer valer, cuando corresponda.
- Dirección física, electrónica y teléfono de contacto del Titular y/o sus causahabientes o representantes;
- Firma, número de identificación o procedimiento de validación correspondiente.
- Haber sido presentada por los medios de consulta habilitados por NGS&O ABOGADOS S.A.S.

Una vez recibida la solicitud, el responsable del tratamiento resolverá la petición de consulta en un plazo máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. 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.

Una vez agotado el trámite de consulta, el Titular o causahabiente podrá elevar queja ante la autoridad local.

8.2. Derechos de quejas y reclamos.

El Titular de los datos puede ejercitar los derechos de reclamo sobre sus datos, mediante un escrito dirigido al correo electrónico ***asistenteadministrativo@ngsoabogados.com***, indicando en el asunto "ejercicio del derecho queja o reclamo", la solicitud deberá contener los siguientes datos:

- Nombres y apellidos del Titular y/o su representante y/o causahabientes;
- Descripción de los hechos y petición en que se concreta la solicitud de corrección, supresión, revocación o inflación.
- Documentos acreditativos de la petición formulada que se quieran hacer valer, cuando corresponda.
- Dirección física, electrónica y teléfono de contacto del Titular y/o sus causahabientes o representantes;
- Firma, número de identificación o procedimiento de validación correspondiente.
- Haber sido presentada por los medios de consulta habilitados por NGS&O ABOGADOS S.A.S.

Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga “reclamo en trámite” y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

El responsable del tratamiento resolverá la petición de consulta en un plazo máximo de quince (15) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender al 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.

Una vez agotado el trámite de reclamo, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

9. Medidas de seguridad

NGS&O ABOGADOS S.A.S., con el fin de cumplir con el principio de seguridad, ha implementado medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Por otra parte, NGS&O ABOGADOS S.A.S., en caso de que requiera suscribir contratos de transmisión, requerirá a los encargados del tratamiento con los que trabaje, la implementación de las medidas de seguridad necesarias, para garantizar la seguridad y confidencialidad de la información en el tratamiento de los datos personales.

A continuación, se exponen las **medidas de seguridad** implantadas por NGS&O ABOGADOS S.A.S., que están recogidas y desarrolladas en este documento (Tablas II, III, IV y V).

Tabla II.

Medidas de seguridad comunes para todo tipo de datos (públicos, semiprivados[1], privados[2], sensibles) y bases de datos (automatizadas, no automatizadas)

Auditoría	Realización periódica, dependiendo de las necesidades de la organización**.**
	Eventuales auditorías extraordinarias por modificaciones sustanciales en los sistemas de información
	Informe de detección de deficiencias y propuesta de correcciones
	Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento.
	Conservación del Informe a disposición de la autoridad
Gestión de documentos y soportes	Medidas tales como, destructora de papel que eviten el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruidos.
	Acceso restringido al lugar donde se almacenan los datos
	Sistema de identificación del tipo de información
	Inventario de los soportes en los que se almacenan bases de datos
	Autorización del responsable para la salida de documentos o soportes por medio físico o electrónico
Control de acceso	Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones, de acuerdo con el rol que desempeña.
	Lista actualizada de usuarios y accesos autorizados, cuando aplique

[1] Dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento interesa al titular y a cierto sector o grupo de personas o a la sociedad en general (Ej. datos financieros y crediticios, dirección, teléfono, correo electrónico,).

[2] Cuando hablamos de datos personales nos referimos a toda aquella información asociada a una persona y que permite su identificación. Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional.

	Autorización escrita del titular de la información para la entrega de sus datos a terceras personas, para evitar el acceso a datos con derechos distintos de los autorizados.
	Concesión, alteración o anulación de permisos por el personal autorizado
Incidencias	Registro de incidencias: tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras.
	Procedimiento de notificación y gestión de incidencias
Personal	Definición de las funciones y obligaciones de los usuarios con acceso a los datos
	Definición de las funciones de control y autorizaciones delegadas por el responsable del tratamiento
	Divulgación entre el personal de las normas y de las consecuencias del incumplimiento de estas
Políticas y Procedimientos	Elaboración e implementación del Manual de obligatorio cumplimiento para el personal
	Contenido mínimo: ámbito de aplicación, medidas y procedimientos de seguridad, funciones y obligaciones del personal, descripción de las bases de datos, procedimiento ante incidencias, identificación de los encargos del tratamiento, entre otros.

Tabla III.
Medidas de seguridad comunes para todo tipo de datos
(públicos, semiprivados, privados, sensibles) según el tipo de bases de datos

Bases de datos no automatizadas			Bases de datos automatizadas	
Archivo	**Almacenamiento de documentos**	**Custodia de documentos**	**Identificación y autenticación**	**Telecomunicaciones**
1. Archivo de documentación, siguiendo procedimientos que garanticen	1. Dispositivos de almacenamiento con mecanismos que impidan el acceso a	1. Deber de diligencia y custodia de la persona a cargo de	1. Identificación personalizada de usuarios para acceder a los sistemas de	1. Acceso a datos mediante redes seguras.

una correcta conservación, localización y consulta y ejercicio de los derechos de los Titulares.	personas no autorizadas.	documentos, durante la revisión o tramitación de estos.	información y verificación de su autorización. 2. Mecanismos de identificación y autenticación; Contraseñas: asignación, caducidad y almacenamiento	

Tabla IV.
Medidas de seguridad para datos según el tipo de bases de datos

Bases de datos automatizadas y no automatizadas		
Auditoría	**Responsable de seguridad**	**Políticas y Procedimientos Habeas Data**
• Auditorías internas o externas. • Eventuales auditorías extraordinarias por modificaciones sustanciales en los sistemas de información. • Informe de detección de deficiencias y propuesta de correcciones. • Análisis y conclusiones del responsable de	• Designación de uno o varios responsables de seguridad, dependiendo de la dinámica de la organización. • Designación de uno o varios encargados del control y la coordinación de las medidas del Manual políticas y procedimientos, dependiendo de la dinámica de la organización. • Prohibición de delegación de la responsabilidad del responsable del tratamiento	• Controles - auditoria, y capacitación al personal.

seguridad y del responsable del tratamiento. • Conservación del Informe a disposición de la autoridad.	en el responsable de seguridad.	

Bases de datos automatizadas			
Gestión de documento y soportes	**Control de acceso**	**Identificación y autenticación**	**Incidencias**
· Registro de entradas y salida de documentos y soportes: fecha, emisor y receptor, número, tipo, de información, forma de envío, responsable de la recepción o entrega.	· Control de acceso al lugar o lugares donde se ubican los sistemas de información.	· Control del acceso no autorizado.	· Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente. · Autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación.

Tabla V.
Medidas de seguridad para datos según el tipo de bases de datos

Bases de datos no automatizadas			
Control de acceso	**Almacenamiento de documentos**	**Copia o reproducción**	**Traslado de documentación**
• Acceso solo para personal autorizado. • Mecanismo de identificación de acceso. • Registro de accesos de usuarios no autorizados.	• Archivadores, armarios u otros ubicados en áreas de protegidas con llaves u otras medidas.	• Solo por usuarios autorizados. • Destrucción que impida el acceso o recuperación de los datos.	• Medidas que impidan el acceso o manipulación de documentos.

Bases de datos automatizadas		
Gestión de documentos y soportes	**Control de acceso**	**Telecomunicaciones**
• Sistema de etiquetado confidencial. • Cifrado de datos. • Control de dispositivos portátiles cuando sean retirados.	• Control de acceso a las bases de datos. • Control del registro de accesos por el responsable de seguridad. Informe mensual. • Conservación de los datos: por el periodo que las leyes impongan.	• Transmisión de datos mediante redes.

9.1. Encargados de seguridad

Los encargados de seguridad tienen las siguientes funciones:

- Coordinar y controlar la implantación de las medidas de seguridad, y colaborar con el responsable del tratamiento en la difusión de la presente Política y Manual.
- Coordinar y controlar los mecanismos que permiten acceder a la información contenida en las bases de datos y elaborar un informe cuando les sea requerido.
- Gestionar los permisos de acceso a los datos por parte de los usuarios autorizados identificados en este documento.
- Habilitar el registro de incidencias a todos los usuarios para que comuniquen y registren las incidencias relacionadas con la seguridad de los datos; así como acordar con el responsable del tratamiento las medidas correctoras y registrarlas.
- Comprobar periódicamente, la validez y vigencia de la lista de usuarios autorizados, la existencia y validez de las copias de seguridad para la recuperación de los datos, la actualización en este manual y el cumplimiento de las medidas relacionadas con las entradas y salidas de datos.
- Definir los tiempos dentro de los cuales se realizarán las auditorias, los cuales NO podrán ser superiores a un año.
- Recibir y analizar el informe de auditoría para elevar sus conclusiones y proponer medidas correctoras al responsable del tratamiento.
- Gestionar y controlar los registros de entradas y salidas de documentos o soportes que contengan datos personales.

9.2. Usuarios

Todas las personas que intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con los datos personales y sistemas de información del responsable del tratamiento, deben actuar de conformidad a las funciones y obligaciones recogidas en el presente apartado.

El responsable del tratamiento cumplirá con el deber de información con su inclusión de acuerdos de confidencialidad y deber de secreto que suscriben, en su caso, los usuarios de sistemas de identificación sobre bases de datos y sistemas de información.

Las funciones y obligaciones del personal del responsable del tratamiento se definen, con carácter general, según el tipo de actividad que desarrollan de acuerdo con sus funciones dentro de la institución y, específicamente, por el contenido de este documento.

Con carácter general, cuando un usuario trate documentos o soportes que contiene datos personales tiene el deber de custodiarlos, así como de vigilar y controlar que personas no autorizadas no puedan tener acceso a ellos.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en este Documento de Políticas y Procedimientos Habeas Data por parte del personal al servicio del responsable del tratamiento, es sancionable de acuerdo con la normativa aplicable a la relación jurídica existente.

Las funciones y obligaciones de los **usuarios** de las bases de datos personales bajo responsabilidad del responsable del tratamiento son las siguientes:

- **Deber de secreto:** Aplica a todas las personas que, en el desarrollo de su profesión o trabajo, acceden a bases de datos personales y vincula tanto a usuarios como a prestadores de servicios contratados; en cumplimiento de este deber, los usuarios del responsable del tratamiento no pueden comunicar o relevar a terceras personas, datos que manejen o de los que tengan conocimiento en el desempeño o cargo de sus funciones, y deben velar por la confidencialidad e integridad de los mismos.

- **Funciones de control y autorizaciones delegadas**: el responsable del tratamiento puede delegar el tratamiento de datos a terceros, para que actúen como encargados del tratamiento, mediante un contrato de transmisión de datos.

- **Obligaciones relacionadas con las medidas de seguridad implantadas:**
  - Acceder a las bases de datos solamente con la debida autorización y cuando sea necesario para el ejercicio de sus funciones.
  - No revelar información a terceras personas ni a usuarios no autorizados.
  - Observar las normas de seguridad y trabajar para mejorarlas.
  - No realizar acciones que supongan un peligro para la seguridad de la información.
  - No sacar información de las instalaciones de la organización sin la debida autorización.

- **Uso de recursos y materiales de trabajo:** debe estar orientado al ejercicio de las funciones asignadas. No se autoriza el uso de estos recursos y materiales para fines personales o ajenos a las tareas correspondientes al puesto de trabajo. Cuando, por motivos justificados de trabajo, sea necesaria la salida de dispositivos periféricos o extraíbles, deberá comunicarse al responsable de seguridad correspondiente que podrá autorizarla y, en su caso, registrarla.

- **Uso de impresoras, escáneres y otros dispositivos de copia:** Cuando se utilicen este tipo de dispositivos debe procederse a la recogida inmediata de las copias, evitando dejar éstas en las bandejas de los mismos.

- **Obligación de notificar incidencias:** Los usuarios tienen la obligación de notificar las incidencias de las que tenga conocimiento al responsable de seguridad que corresponda, quien se encargará de su gestión y resolución. Algunos ejemplos de incidencias son: la caída del sistema de seguridad informática que permita el acceso a los datos personales a personas no autorizadas, el intento no autorizado de la salida de un documento o soporte, la pérdida de datos o la destrucción total o parcial de soportes, el cambio de ubicación física de bases de datos, el conocimiento por terceras personas de contraseñas, la modificación de datos por personal no autorizado, etc.

- **Deber de custodia de los soportes utilizados:** obliga al usuario autorizado a vigilar y controlar que personas no autorizadas accedan a la información contenida en los soportes. Los soportes que contienen bases de datos deben identificar el tipo de información que contienen.

- **Responsabilidad sobre los terminales de trabajo y portátiles:** cada usuario es responsable de su propio terminal de trabajo; cuando esté ausente de su puesto, debe bloquear dicho terminal (ej. protector de pantalla con contraseña) para impedir la visualización o el acceso a la información que contiene; y tiene el deber de apagar el terminal al finalizar la jornada laboral. Asimismo, los ordenadores portátiles han de estar controlados en todo momento para evitar su pérdida o sustracción.

- **Uso limitado de Internet y del correo electrónico:** El envío de información por vía electrónica y el uso de Internet por parte del personal está limitado al desempeño de sus actividades.

- **Salvaguarda y protección de contraseñas:** Las contraseñas proporcionadas a los usuarios son personales e intransferibles, por lo que se prohíbe su divulgación o comunicación a personas no autorizadas. Cuando el usuario accede por primera vez con la contraseña asignada es necesario que la cambie. Cuando sea necesario restaurar la contraseña, el usuario debe comunicarlo al administrador del sistema.

- **Copias de respaldo y recuperación de datos:** debe realizarse copia de seguridad de toda la información de bases de datos personales de la institución.

- **Deber de archivo y gestión de documentos y soportes:** Los documentos y soportes deben de ser debidamente archivados con las medidas de seguridad recogidas en este manual.

10. Transferencia de datos a terceros países.

Se prohíbe la transferencia de datos personales a países que no proporcionen niveles adecuados de protección de datos. Esta prohibición no regirá cuando se trate de:

- Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.
- Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del Titular por razones de salud o higiene pública.
- Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.
- Transferencias acordadas en el marco de tratados internacionales, con fundamento en el principio de reciprocidad.
- Transferencias necesarias para la ejecución de un contrato entre el Titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.
- Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

En los casos no contemplados como excepción, corresponderá a la Autoridad Local proferir la declaración de conformidad relativa a la transferencia internacional de datos personales.

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, siempre que exista un **contrato de transmisión** de datos personales.

CAPITULO II
DE LAS MEDIDAS DE SEGURIDAD

1. Cumplimiento y actualización.

Este es un documento interno de obligatorio cumplimiento para todo el personal de NGS&O ABOGADOS S.A.S., con acceso a los sistemas de información que contengan datos personales. Teniendo en cuenta que NGS&O ABOGADOS S.A.S. cuenta con una Política de Seguridad de la Información general, las presentes medidas deben entenderse como aplicables, exclusivamente, para la protección de datos personales y prevalecerán en todo lo que riña con las políticas generales.

Este manual de Políticas y Procedimientos Habeas Data, debe ser sometido a permanente revisión y actualización siempre que se produzcan cambios en los sistemas

de información, el sistema de tratamiento, la organización o el contenido de la información de las bases de datos, que puedan afectar a las medidas de seguridad implementadas. Asimismo, el manual debe adaptarse en todo momento a la normativa legal en materia de seguridad de datos personales.

2. Medidas de seguridad.

Las bases de datos son accesibles únicamente por las personas designadas por el responsable del tratamiento, y referidas en este documento.

Los responsables de seguridad, señalados en el presente manual, se encargan de gestionar los permisos de acceso a los usuarios, el procedimiento de asignación y distribución que garantiza la confidencialidad, integridad y almacenamiento de las contraseñas, durante su vigencia, así como la periodicidad con la que se cambian.

A continuación, se enumeran y detallan las medidas de seguridad implementadas por el responsable del tratamiento

2.1 Medidas de seguridad comunes.

2.1.1 Gestión de documentos y soportes.

Los documentos y soportes en los que se encuentran las bases de datos se determinan en el inventario de documentos y soportes.

Los encargados de vigilar y controlar que personas no autorizadas no puedan acceder a los documentos y soportes con datos personales son los usuarios autorizados para acceder a estos. Los usuarios autorizados están referidos en el presente manual.

Los documentos y soportes deben clasificar los datos según el tipo de información que contienen, ser inventariados y ser accesibles solo por el personal autorizado, salvo que las características de estos hagan imposible la identificación referida, en cuyo caso se dejará constancia motivada en el registro de entrada y de salida de documentos y en este manual.

La salida de documentos y soportes que contengan datos personales fuera de los locales que están bajo el control del responsable del tratamiento debe ser autorizada por este último. Este precepto también es aplicable a los documentos o soportes anexados y enviados por correo electrónico.

El **inventario de documentos** y soportes del responsable del tratamiento, deben incluirse como anexo del presente manual.

3. Control de acceso.

El personal del responsable del tratamiento solamente debe acceder a aquellos datos y recursos necesarios para el desarrollo de sus funciones y sobre los cuales se encuentren autorizados por el responsable del tratamiento en este manual.

El responsable del tratamiento se ocupa del almacenamiento de una lista actualizada de usuarios, perfiles de usuarios, y de los accesos autorizados para cada uno de ellos. Además, tiene mecanismos para evitar el acceso a datos con derechos distintos de los autorizados. En el caso de soportes informáticos, puede consistir en la asignación de contraseñas, y en el caso de documentos, en la entrega de llaves o mecanismos de apertura de dispositivos de almacenamiento donde se archive la documentación.

La modificación sobre algún dato o información, así como la concesión, alteración, inclusión o anulación de los accesos autorizados y de los usuarios recogidos en la lista actualizada mencionada en el párrafo anterior, corresponde de manera exclusiva al personal autorizado.

Cualquier personal ajeno el responsable del tratamiento que, de forma autorizada y legal, tenga acceso a los recursos protegidos, estará sometido a las mismas condiciones y tendrá las mismas obligaciones de seguridad que el personal propio.

Los usuarios autorizados para el acceso a las bases de datos se establecen en este manual.

3.1 Ejecución del tratamiento fuera de la institución.

El almacenamiento de datos personales del responsable del tratamiento o encargado del tratamiento en dispositivos portátiles y su tratamiento fuera del lugar natural de trabajo, requiere una autorización previa por parte del responsable del tratamiento, y el cumplimiento de las garantías de seguridad correspondientes al tratamiento de este tipo de datos.

3.2 Bases de datos temporales, copias y reproducciones.

Las bases de datos temporales o copias de documentos creadas para trabajos temporales o auxiliares deben cumplir con el mismo nivel de seguridad que corresponde

a las bases de datos o documentos originales. Una vez que dejan de ser necesarias, estas bases de datos temporales o copias son borradas o destruidas, impidiéndose así el acceso o recuperación de la información que contienen.

Solamente el personal autorizado en el **numeral 12** puede realizar copias o reproducir los documentos.

3.3 Responsable de seguridad.

De acuerdo con la normativa sobre protección de datos, la designación de los responsables de seguridad no exonera de responsabilidad al responsable del tratamiento o encargado del tratamiento.

4. Auditoría.

Las bases de datos que contengan datos personales, objeto de tratamiento por el responsable del tratamiento, clasificadas con nivel de seguridad sensible o privado, se podrán someter a una auditoría, con una periodicidad no inferior a los 12 meses, esta puede ser una auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad contenidas en este manual.

El responsable del tratamiento realizará una auditoría extraordinaria siempre que se realicen modificaciones sustanciales en el sistema de información que puedan afectar al cumplimiento de las medidas de seguridad, con el fin de verificar la adaptación, adecuación y eficacia de estas.

5. Medidas de seguridad para bases de datos no automatizadas.

5.1 Archivo de documentos.

El responsable del tratamiento fija los criterios y procedimientos de actuación que se deben utilizar para el archivo de documentos que contengan datos personales conforme a la Ley. Los criterios de archivo garantizan la conservación, localización y consulta de los documentos y hacen posible los derechos de consulta y reclamo de los Titulares. Estos criterios y procedimientos se recogen en este manual.

Se recomienda que los documentos sean archivados considerando, entre otros, criterios como el grado de utilización de los usuarios con acceso autorizado a los mismos, la actualidad de su gestión y/o tratamiento y la diferenciación entre bases de datos históricas y de administración o gestión de la institución.

Los dispositivos de almacenamiento de documentos deben disponer de llaves u otros mecanismos que dificulten su apertura, excepto cuando las características físicas de éstos lo impidan, en cuyo caso el responsable del tratamiento adoptará las medidas necesarias para impedir el acceso de personas no autorizadas.

Cuando los documentos que contienen datos personales se encuentren en proceso de revisión o tramitación y, por tanto, fuera de los dispositivos de almacenamiento, ya sea antes o después de su archivo, la persona que se encuentre a cargo de estos debe custodiarlos e impedir en todo caso que personas no autorizadas puedan acceder a ellos.

Los dispositivos de almacenamiento que contengan documentos con datos personales clasificados con nivel de seguridad sensible**,** deben encontrarse en áreas o locales en las que el acceso esté protegido con puertas de acceso con sistemas de apertura de llave u otros mecanismos similares. Estas áreas deben permanecer cerradas cuando no se precise el acceso a dichos documentos. Si no fuera posible cumplir con lo anterior, el responsable del tratamiento podrá adoptar medidas alternativas debidamente motivadas que se incluirán en el presente documento.

La descripción de las medidas de seguridad de almacenamiento de encuentran recogidas en este documento y en la Política de Seguridad de la Información de NGS&O ABOGADOS S.A.S.

6. Acceso a los documentos.

El acceso a los documentos ha de realizarse exclusivamente por el personal autorizado, siguiendo los mecanismos y procedimientos definidos. Estos últimos deben identificar y conservar los accesos realizados a la documentación clasificada.

El procedimiento de acceso a los documentos que contienen datos implica el **registro de accesos a la documentación**, la identidad de quien accede, el momento en que se produce el acceso y los documentos a los que se han accedido. El acceso a documentos con este tipo de datos se realiza por personal autorizado; si se realiza por **personas no autorizadas** deberá supervisarse por algún usuario autorizado o por el responsable de seguridad en cuestión.

7. Medidas de seguridad para bases de datos automatizadas.

7.1 Identificación y autenticación.

El responsable del tratamiento debe instalar un sistema de seguridad informática que permita identificar y autenticar de forma correcta a los usuarios de los sistemas de información, con el fin de garantizar que solo el personal autorizado pueda acceder a la información.

También ha de establecer un mecanismo que permita la identificación personalizada e inequívoca de todo usuario que intente acceder al sistema de información y que verifique si está autorizado. La identificación debe realizarse mediante un sistema único para cada usuario que accede a la información teniendo en cuenta el nombre de usuario, la identificación de empleado, el nombre del departamento, etc.

Cuando el sistema de autenticación esté basado en la introducción de contraseña, se ha de implantar un procedimiento de asignación, distribución y almacenamiento de contraseñas; para garantizar la integridad y confidencialidad de estas últimas, se recomiendan que tengan un mínimo de ocho caracteres y contengan mayúsculas, minúsculas, números y letras. se regirá de acuerdo a la Política interna de Seguridad de la Información y Ciberseguridad que establece los lineamientos respecto a las contraseñas de los usuarios.

El responsable del tratamiento también garantiza el almacenamiento automatizado interno de las contraseñas mientras estén vigentes.

8. Copias de respaldo y recuperación de datos.

El responsable del tratamiento realizará los procedimientos de actuación necesarios para realizar copias de respaldo, excepto cuando no se haya producido ninguna actualización de los datos. Todas las bases de datos deben tener una copia de respaldo a partir de las cuales se puedan recuperar los datos.

De igual modo, ha establecido procedimientos para la recuperación de los datos con el objetivo de garantizar en todo momento la reconstrucción al estado en el que éstos se encontraban, antes de su pérdida o destrucción. Cuando la pérdida o destrucción afecte a bases de datos parcialmente automatizadas, se grabarán manualmente los datos dejando constancia de ello en este manual.

El responsable del tratamiento se encargará de controlar el correcto funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos.

NGS&O ABOGADOS S.A.S. debe conservar una copia de respaldo de los datos y de los procedimientos de recuperación de estos, en un lugar distinto a aquel en el que se encuentren los equipos donde se lleva a cabo su tratamiento. Este lugar deberá cumplir, en todo caso, con las mismas medidas de seguridad exigidas para los datos originales.

9. Registro de acceso.

De los intentos de acceso a los sistemas de información del responsable del tratamiento deberá guardar, como mínimo, la identificación del usuario, la fecha y hora en que se lleva a cabo, la base de datos a la que se accede, el tipo de acceso y si ese acceso ha sido autorizado o no autorizado. En caso de que el registro haya sido autorizado, se guarda la información que permita identificar el registro consultado.

Los responsables de seguridad de las bases de datos automatizadas, se encargan de controlar los mecanismos que permiten el registro de acceso, revisar con carácter mensual la información de control registrada y elaborar un informe de las revisiones realizadas y los problemas detectados. Además, deben impedir la manipulación o desactivación de los mecanismos que permiten el registro de acceso.

Los datos que contiene el registro de acceso deben conservarse, al menos, durante dos años.

No será necesario el registro de acceso, cuando el responsable del tratamiento sea una persona natural y garantice que solamente él tiene acceso y trata los datos personales.

El acceso a datos personales a través de redes de comunicaciones, públicas o privadas, debe someterse a medidas de seguridad equivalentes al acceso local de datos personales.

La transmisión o transferencia de datos personales mediante redes públicas o inalámbricas de comunicaciones electrónicas se tiene que llevar a cabo cifrando dichos datos, o utilizando otro mecanismo similar que garantice que la información no sea inteligible ni manipulada por terceras personas.

10. Funciones y obligaciones del personal

Todas las personas que intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con los datos personales y sistemas de información, deben actuar de conformidad a las funciones y obligaciones recogidas en el presente apartado.

NGS&O ABOGADOS S.A.S. debe informar a su personal de servicio de las medidas y normas de seguridad que compete al desarrollo de sus funciones, así como de las consecuencias de su incumplimiento, mediante cualquier medio de comunicación que garantice su recepción o difusión (correo electrónico, tablón de anuncios, etc.). De igual modo, debe poner a disposición del personal el presente documento de Políticas y Procedimientos Habeas Data para que puedan conocer la normativa de seguridad y sus obligaciones en esta materia en función del cargo que ocupan.

NGS&O ABOGADOS S.A.S. cumple con el deber de información con su inclusión de **acuerdos de confidencialidad** que suscriben, en su caso, los usuarios de sistemas de identificación referidos en el **numeral 12** sobre bases de datos y sistemas de información.

Las funciones y obligaciones del personal de NGS&O ABOGADOS S.A.S. se definen, con carácter general, según el tipo de actividad que desarrollan al interior de la institución, específicamente, por el contenido de este manual. La lista de usuarios y perfiles con acceso a los recursos protegidos están recogidos en el **numeral 12** sobre bases de datos y sistemas de información. Con carácter general, cuando un usuario trate documentos o soportes que contiene datos personales tiene el deber de custodiarlos, así como de vigilar y controlar que personas no autorizadas no puedan tener acceso a ellos.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente manual, por parte del personal al servicio del responsable del tratamiento es sancionable de acuerdo con la normativa aplicable a la relación jurídica existente entre las partes.

Las funciones y obligaciones de los usuarios de las bases de datos personales, bajo responsabilidad del responsable del tratamiento son las siguientes:

- **Deber de secreto**: Aplica a todas las personas que, en el desarrollo de su profesión o trabajo, acceden a bases de datos personales y vincula tanto a usuarios como a prestadores de servicios contratados; en cumplimiento de este deber, los usuarios de la organización no pueden comunicar o relevar a terceras personas, datos que manejen o de los que tengan conocimiento en el desempeño o cargo de sus funciones, y deben velar por la confidencialidad e integridad de estos.
- **Funciones de control y autorizaciones delegadas**: El responsable del tratamiento puede delegar el tratamiento de datos a terceros, para que actúe como encargado del tratamiento, mediante un contrato de transmisión de datos.

Las obligaciones relacionadas con las medidas de seguridad implantadas:

- Acceder a las bases de datos solamente con la debida autorización y cuando sea necesario para el ejercicio de sus funciones.
- No revelar información a terceras personas ni a usuarios no autorizados. Observar las normas de seguridad y trabajar para mejorarlas.
- No realizar acciones que supongan un peligro para la seguridad de la información.
- No extraer información de las instalaciones de la organización sin la debida autorización.
- Uso de recursos y materiales de trabajo: debe estar orientado al ejercicio de las funciones asignadas.
- No se autoriza el uso de estos recursos y materiales para fines personales o ajenos a las tareas correspondientes al puesto de trabajo. Cuando, por motivos justificados de trabajo, sea necesaria la salida de dispositivos periféricos o extraíbles, deberá comunicarse a los responsables de seguridad que podrán autorizarla y, en su caso, registrarla.
- Uso de impresoras, escáneres y otros dispositivos de copia: cuando se utilicen este tipo de dispositivos, debe procederse a la recogida inmediata de las copias, evitando dejar éstas en las bandejas de estos.
- Obligación de notificar incidencias: los usuarios tienen la obligación de notificar las incidencias de las que tenga conocimiento a los responsables de seguridad, quienes se encargarán de su gestión y resolución. Algunos ejemplos de incidencias son: la caída del sistema de seguridad informática que permita el acceso a los datos personales a personas no autorizadas, el intento no autorizado de la salida de un documento o soporte, la pérdida de datos o la destrucción total o parcial de soportes, el cambio de ubicación física de bases de datos, el conocimiento por terceras personas de contraseñas, la modificación de datos por personal no autorizado, etc.
- Deber de custodia de los soportes utilizados: obliga al usuario autorizado a vigilar y controlar que personas no autorizadas accedan a la información contenida en los soportes.
- Responsabilidad sobre los terminales de trabajo y portátiles: Cada usuario es responsable de su propio terminal de trabajo; cuando esté ausente de su puesto, debe bloquear dicho terminal (ej. protector de pantalla con contraseña) para impedir la visualización o el acceso a la información que contiene; y tiene el deber de apagar el terminal al finalizar la jornada laboral. Asimismo, los ordenadores portátiles han de estar controlados en todo momento para evitar su pérdida o sustracción.

- Uso limitado de Internet y del correo electrónico: El envío de información por vía electrónica y el uso de Internet por parte del personal, está limitado al desempeño de sus actividades.
- Salvaguarda y protección de contraseñas: Las contraseñas proporcionadas a los usuarios son personales e intransferibles, por lo que se prohíbe su divulgación o comunicación a personas no autorizadas. Cuando el usuario accede por primera vez con la contraseña asignada es necesario que la cambie. Cuando sea necesario restaurar la contraseña, el usuario debe comunicarlo al administrador del sistema.
- Copias de respaldo y recuperación de datos: Debe realizarse copia de seguridad de toda la información de bases de datos personales propiedad del responsable del tratamiento.
- Deber de archivo y gestión de documentos y soportes: Los documentos y soportes deben de ser debidamente archivados, con las medidas de seguridad establecidas en el presente capítulo.

11. Bases de datos y sistemas de información.

Las bases de datos almacenadas y tratadas por NGS&O ABOGADOS S.A.S. se recogen en la siguiente tabla (Tabla I), donde se indica el nivel de seguridad y el sistema de tratamiento de cada una de ellas.

Tabla I. Bases de datos y nivel de seguridad

Bases de Datos	Nivel de Seguridad
Empleados, practicantes, candidatos a vacantes	Medio

Bases de Datos	Nivel de Seguridad
Proveedores de bienes y servicios	Medio

Bases de Datos	Nivel de Seguridad
Clientes y Clientes Potenciales	Medio

Bases de Datos	Nivel de Seguridad
Accionistas y Administradores	**Alto**

CLASIFICACION	OBSERVACIONES	NIVEL DE PROTECCION	PERFIL
Confidencial	Información propia de la sociedad, acceso a sistemas de información, acceso a bases de datos de Accionistas y Administradores, manuales operativos, configuración de controles, sistemas de protección y seguridad e información de cumplimiento de la ley.	Alto	NIVEL 1
Restringida	Acceso a las siguientes bases de datos: Empleados, practicantes, candidatos a vacantes / Proveedores de bienes y servicios / Clientes y clientes potenciales / que solo debe ser accedida por personal autorizado para ello, previa autorización del dueño del proceso.	Medio	NIVEL 2

La siguiente tabla (Tabla II) recoge la estructura de las bases de datos de NGSO ABOGADOS S.A.S.**:**

Tabla II. Estructura de las Bases de datos

Nombre de la base de datos	Empleados, practicantes, candidatos a vacantes
Responsable del tratamiento	NGSO ABOGADOS S.A.S.
Encargado de consultas y reclamos	Representante legal
Tipo de datos	Básicos, privados, semiprivados y sensibles
Control de acceso físico	Usuarios Autorizados
Control de acceso lógico	Usuarios y contraseñas
Copias de respaldo	Mensual

Nombre de la base de datos	Proveedores de bienes y servicios
Responsable del tratamiento	NGSO ABOGADOS S.A.S.
Encargado de consultas y reclamos	Representante legal
Tipo de datos	Básicos, privados, semiprivados y sensibles
Control de acceso físico	Usuarios Autorizados
Control de acceso lógico	Usuarios y contraseñas
Copias de respaldo	mensual

Nombre de la base de datos	Clientes y Clientes Potenciales
Responsable del tratamiento	NGSO ABOGADOS S.A.S.
Encargado de consultas y reclamos	Representante legal
Tipo de datos	Básicos, privados, semiprivados y sensibles
Control de acceso físico	Usuarios Autorizados
Control de acceso lógico	Usuarios y contraseñas
Copias de respaldo	Mensual

Nombre de la base de datos	Accionistas y Administradores
Responsable del tratamiento	NGSO ABOGADOS S.A.S.
Encargado de consultas y reclamos	Representante legal
Tipo de datos	Básicos, privados, semiprivados y sensibles
Control de acceso físico	Usuarios Autorizados
Control de acceso lógico	Usuarios y contraseñas
Copias de respaldo	Mensual

El nombramiento de los responsables de seguridad, no exonera al responsable del tratamiento o al encargado del tratamiento de sus obligaciones.

Cuando exista contrato de transmisión de datos, los encargados del tratamiento se identificarán en el Registro de contratos de transmisión de datos de este documento. Los encargados del tratamiento deberán cumplir con las funciones y obligaciones relacionadas con las medidas en materia de seguridad recogidas en el presente manual.

11.1 Procedimiento de notificación, gestión y respuesta ante incidencias

NGS&O ABOGADOS S.A.S. establece un procedimiento de notificación, gestión y respuesta de incidencias con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información contenida en las bases de datos que están bajo su responsabilidad.

Todos los usuarios y responsables de procedimientos, así como cualquier persona que tenga relación con el almacenamiento, tratamiento o consulta de las bases de datos recogidas en este documento, deben conocer el procedimiento para actuar en caso de incidencia.

El procedimiento de notificación, gestión y respuesta ante incidencias es el siguiente:

- Cuando una persona tenga conocimiento de una incidencia que afecte o pueda afectar la confidencialidad, disponibilidad e integridad de la información protegida de la institución deberá comunicarlo, de manera inmediata, a los responsables de seguridad, describiendo detalladamente el tipo de incidencia producida, e indicando las personas que hayan podido tener relación con la incidencia, la fecha y hora en que se ha producido, la persona que notifica la incidencia, la persona a quién se le comunica y los efectos que ha producido.

- Una vez comunicada la incidencia, ha de solicitar al responsable de seguridad correspondiente un acuse de recibo en el que conste la notificación de la incidencia, con todos los requisitos enumerados anteriormente.

NGS&O ABOGADOS S.A.S. crea un registro de incidencias que debe contener: el tipo de incidencia, fecha y hora de esta, persona que la notifica, persona a la que se le comunica, efectos de la incidencia y medidas correctoras cuando corresponda. Este registro es gestionado por el responsable de seguridad de la base de datos y debe incluirse como anexo en el presente manual.

Asimismo, debe implementar los procedimientos para la recuperación de los datos, indicando quien ejecuta el proceso, los datos restaurados y, en su caso, los datos que han requerido ser grabados manualmente en el proceso de recuperación.

11.2 Reporte

Todos los incidentes y eventos sospechosos deben ser reportados tan pronto como sea posible, a través de los canales internos establecidos; Si la información sensible o

confidencial es perdida, divulgada a personal no autorizado o se sospecha de alguno de estos eventos, el responsable de la información debe ser notificado de forma inmediata. Los funcionarios deben reportar a su jefe directo y/o al Oficial de Protección de Datos Personales, cualquier daño o pérdida de computadores o cualquiera otro dispositivo, cuando estos contengan datos personales en poder de la Entidad. A menos que exista una solicitud de la autoridad competente debidamente razonada y justificada, ningún funcionario debe divulgar información sobre sistemas de cómputo, y redes que hayan sido afectadas por un delito informático o abuso de sistema. Para la entrega de información o datos en virtud de orden de autoridad, el área jurídica deberá intervenir con el fin de prestar el asesoramiento adecuado.

El responsable de la información debe garantizar que se tomen acciones para investigar y diagnosticar las causas que generaron el incidente, así como también debe garantizar que todo el proceso de gestión del incidente sea debidamente documentado, apoyado con la Oficina de Tecnologías e Informática.

12. Medidas para el transporte, destrucción y reutilización de documentos y soportes.

Cuando corresponda desechar cualquier documento (original, copia o reproducción) o soporte que contenga datos personales, debe procederse a su destrucción o borrado, a través de la implementación de medidas orientadas a evitar el acceso o recuperación de la información contenida en dicho documento o soporte.

Antes de iniciar la destrucción, se realizará un acta o se llevará el registro a través de cualquier medio, físico o digital; en dicha anotación se describirá el documento objeto de destrucción, la fecha, hora y firma de dos personas que evidencian la destrucción.

Cuando se lleve a cabo el traslado físico de documentos o soportes deben adoptar las medidas necesarias para impedir el acceso indebido, la manipulación, la sustracción o la pérdida de la información. El traslado de soportes que contengan datos personales se realiza cifrando la información, o utilizando cualquier otro mecanismo que garantice que no se manipule ni se acceda a la misma.

Los datos personales contenidos en dispositivos portátiles, deben estar controlados cuando se hallen fuera de las instalaciones que están bajo control de NGS&O ABOGADOS S.A.S.; Cuando no sea posible el control, se debe evitar el tratamiento de datos personales mediante este tipo de dispositivos; sin embargo, se podrá proceder al tratamiento cuando sea estrictamente necesario, adoptando para ello medidas de seguridad que tengan en cuenta los riesgos e incluyéndolas en el presente manual.

13. Infracciones y sanciones

Las autoridades locales pueden imponer sanciones por el incumplimiento de la normativa sobre protección de datos al responsable del tratamiento o al encargado del tratamiento. Estas se encuentran en la normativa vigente y pueden variar dependiendo de la violación.

14. Vigencia

Las bases de datos responsabilidad de NGS&O ABOGADOS S.A.S., serán objeto de tratamiento durante el tiempo que sea razonable y necesario para la finalidad para la cual son recabados los datos. Una vez cumplida la finalidad o finalidades del tratamiento, y sin perjuicio de normas legales que dispongan lo contrario, se procederá a la supresión de los datos personales en su posesión, salvo que exista una obligación legal o contractual que requiera su conservación. Por todo ello, el presente documento entra en vigencia a partir de su expedición.