OBJETIVO:
Garantizar el adecuado tratamiento de datos sensibles de las partes interesadas como empleados, accionistas, directivos, clientes y proveedores que sean de alcance de APOLO GROUP S.A.S. Así mismo tiene la finalidad de regular los procedimientos de recolección, manejo y tratamiento de los datos de carácter personal que realiza APOLO GROUP S.A.S, a fin de garantizar y proteger el derecho fundamental de habeas data en el marco de lo establecido en la misma ley.

ALCANCE:
Desde la recepción de la información, hasta el procesamiento y entrega a las partes interesadas, en los casos que APOLO GROUP S.A.S actúe como responsable o encargado del tratamiento.
Los controles descritos en este documento, responden a los requisitos exigidos por Ley 1581 de 2012, decreto 1377 de 2013 y Ley 1266 de habeas data.

DEFINICIONES:

a) **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;

b) **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;

c) **Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento;

d) **Causa habitante:** es aquella persona física o jurídica que se ha sucedido o sustituido a otra

e) **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales; medios por los cuales APOLO GROUP S.A.S va a solicitar la autorización interna y de terceros

f) **Aviso de privacidad:** Documento físico, electrónico o en cualquier otro formato generado por el Responsable que se pone a disposición del Titular para el tratamiento de sus datos personales. En el Aviso de Privacidad se comunica al Titular la información relativa a la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las características del tratamiento que se pretende dar a los datos personales.

g) **Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento.

h) **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varia personas naturales determinadas o determinables;

i) **Dato privado:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

j) **Datos sensibles:** Se entiende por datos sensibles 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.

k) **Agencia de Información Comercial.** Es toda empresa legalmente constituida que tenga como actividad principal la recolección, validación y procesamiento de información comercial sobre las empresas y comerciantes específicamente solicitadas por sus clientes, entendiéndose por información comercial aquella información histórica y actual relativa a la situación financiera, patrimonial, de mercado, administrativa, operativa, sobre el cumplimiento de obligaciones y demás información relevante para analizar la situación integral de una empresa. Las agencias de información comercial son operadores de información y fuentes de información.

l) **Habeas data:** Es el derecho que tienen todas las personas (titulares) a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.

m) **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión de los mismos.

n) **Transferencia:** La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

o) **Transmisión:** Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable.

p) Recolección: Etapa de obtención de datos para conseguir la información necesaria que permitirá llevar a cabo la finalidad indicada.

q) Almacenamiento: Sistema ordenado que permite guardar física o virtualmente archivos de datos.

r) Uso y circulación: Tratamiento dado a los datos recolectados y almacenados, conforme a la finalidad señalada e informada al titular del dato.

CONTENIDO:

PRINCIPIOS. Los principios que se establecen a continuación, constituyen los parámetros generales que serán respetados por APOLO GROUP S.A.S en los procesos de recolección, uso, almacenamiento y circulación o supresión de datos personales.

a) **Principio de legalidad**: El Tratamiento a datos personas que realice APOLO GROUP S.A.S antes, durante y posterior a la relación, cumple a las disposiciones de ley.

b) **Principio de finalidad:** Todo tratamiento de los datos personales recogidos por APOLO GROUP S.A.S obedecen al desarrollo de las actividades propias del negocio, la cual debe garantizar la autorización del Titular.

c) **Principio de libertad:** El Tratamiento sólo puede llevarse a cabo con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

d) **Principio de veracidad o calidad:** La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error. Anualmente el responsable de la Base de datos, debe garantizar su actualización.

e) **Principio de transparencia:** En cualquier momento y sin restricciones el Titular puede solicitar a APOLO GROUP S.A.S, información acerca de la existencia de datos que le conciernan.

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

g) **Principio de seguridad:** La información sujeta a Tratamiento por parte de APOLO GROUP S.A.S, es protegida a través del uso de medidas técnicas, humanas y administrativas que son necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; adicional se acompaña con todos los lineamientos definidos en la Política de Seguridad de la Compañía.

h) **Principio de confidencialidad:** Todas las personas que intervengan en el Tratamiento de datos personales están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento. Para todas las relaciones contractuales se define la firma del anexo de Seguridad de la Información para todas las partes interesadas.

RESPONSABILIDADES COMUNES ENTRE EL ENCARGADO Y EL RESPONSABLE DEL TRATAMIENTO:

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) Tramitar las consultas y reclamos frente a la protección de datos, a los que pueda verse expuesta la Compañía.
d) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la protección de datos y en especial, para la atención de consultas y reclamos.
e) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

RESPONSABILIDADES DEL RESPONSABLE DEL TRATAMIENTO:

a) Solicitar y conservar copia de la respectiva autorización otorgada por el Titular.
b) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que tiene según la autorización otorgada.
c) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
d) 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.
e) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.

f) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la ley 1581 – protección de datos.
g) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
h) 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.
i) Informar a solicitud del Titular sobre el uso dado a sus datos.
j) 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.

RESPONSABILIDADESDE EL ENCARGADO DEL TRATAMIENTO:

a) Realizar oportunamente la actualización, rectificación o supresión de los datos
b) Actualizar la información reportada por los Responsables del Tratamiento dentro de los **cinco (5) días hábiles** contados a partir de su recibo.
c) Registrar en la base de datos la leyenda "reclamo en trámite" hasta que se solucionen
d) 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.
e) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
f) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
g) Informar a la Superintendencia de Industria y Comercio cuando se le presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

POLÍTICAS:

APOLO GROUP S.A.S dentro de sus facultades, garantiza la seguridad de la información, por lo cual es compromiso de cada uno de los empleados, asegurar la seguridad de la información sensible, personal y confidencial de todas las partes: clientes, proveedores, empleados, entre otros.

La información a la cual se tenga acceso sólo será usada para el fin definido en la relación comercial o laboral a la que se comprometan las partes.

El área de Comunicaciones y/o Mercadeo sólo podrán enviar información con datos sensibles o personales con la debida autorización por el titular.

Cualquier persona dueña de la información podrá realizar la consulta o supresión de sus datos en el momento en que lo requiera.

Cualquier incumplimiento en la protección de datos sensibles de nuestros empleados, clientes, proveedores o cualquier otro tercero a la que podamos tener acceso, se interpondrán sanciones de acuerdo a lo establecido por el Reglamento interno de trabajo y/o establecido por la ley de Protección de datos.

La compañía debe garantizar la correcta clasificación de la información, pues de acuerdo a esto será su tratamiento. Para esto, dentro de la información que maneja define una categoría para la generación de accesos a los registros, de la siguiente forma:

CLASIFICACIÓN	DESCRIPCIÓN
1. CONFIDENCIAL	Aplica a un grupo directivo o a un grupo interdisciplinario reducido de personas. Esta información es altamente sensible y su filtración genera riesgos de cara a cliente, reputaciones, jurídicos, entre otros.
2. PRIVADO	Grupo o equipo definido por proceso, área o interrelación.
3. RESTRINGIDO	Grupo o equipo definido por proceso, área o interrelación, más un tercero (uno o más personas, definiendo el rol de cada uno).
4. INTERNO	Toda la Organización.
5. PÚBLICO	Toda la organización, más cualquier parte interesada.

En cuanto al dato, se tiene la siguiente clasificación:

CLASIFICACIÓN	DESCRIPCIÓN
Dato personal	Es cualquier información de cualquier tipo, vinculada o que pueda asociarse a una o varias personas determinadas o determinables. Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional. Existe también información más sensible como su estado de salud, sus características físicas, ideología política, vida sexual, entre otros aspectos.
Dato sensible	Es el Dato Personal que afecta la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen afiliaciones sindicales, el origen racial o étnico, la orientación política, las convicciones religiosas, morales 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
Público	Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio ya 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

ASPECTOS GENERALES PARA EL TRATAMIENTO DE DATOS PERSONAL

3. RECOLECCIÓN:

3.1. <u>Bases de datos personales:</u>

De acuerdo al servicio que se preste desde las diferentes líneas de negocio, se defina los datos sensibles/personales a los que se pueda tener acceso o que son administrados por APOLO GROUP S.A.S.

A continuación se describe la información que puede llegar hacer manejada dependiendo del tipo de servicio o proceso en la compañía:

a. *Gestión de Infraestructura de TI:* Por el alcance de este servicio, se puede llegar a tener acceso a información personal y/o sensible de nuestros clientes por medio de la administración de bases de datos con información general y/o sensible.
b. *Gestión de Información:* Bases de datos con la información de los pacientes (cédula, nombre, salario) y resultados de exámenes que se realizan a través de las empresas de salud a las que se le presta el servicio de GI. Adicional se tiene acceso a bases de datos clientes prospecto de nuestros Clientes.
c. *Servicio a Usuario Final:* Por tener servicios asociados de mesas de ayuda de TI o puntos únicos de contacto, se puede tener acceso no sólo de lectura sino también de edición a información como: Cédula de Ciudanía, Estado Civil, Teléfono Personal, Dirección, Estado Civil y/o bases de datos que pueda tener el cliente al cual se le presta soporte.
d. *PILA: Nombre,* Cédula, dirección, salario, pagos a la seguridad social.
e. *Cesantías: Nombre,* Cédula, dirección, salario, pagos a la seguridad social.
f. *Libranzas: Nombre,* Cédula, dirección, salario.

Adicional desde las áreas de apoyo como:

a. *Gestión Humana:*
   Se tiene acceso a datos como: Nacionalidad, Tipo Identificación, Número identificación, Municipio de expedición, fecha expedición, nombre completo, sexo, fecha de nacimiento, dirección residencia, teléfono residencia, ciudad residencia, departamento residencia, celular personal, correo electrónico personal, AFP, EPS, caja de compensación referencias laborales, referencias personales, estudios, instituciones donde estudio, fecha de inicio y fecha final de estudios, grupo familiar, fecha de ingreso a la empresa, cargo, correo electrónico laboral, evaluación de desempeño, jefe inmediato, celular laboral, municipio laboral, departamento laboral, incapacidades, detalle de accidentes, historia clínica (en algunos casos), entre otros.
b. *Abastecimiento:* Se puede tener acceso a información de nuestros proveedores y sus representantes legales tales como: Nombre, Cédula, Certificado bancario, Cámara de Comercio
c. *Mercadeo, Fidelización y Servicio y/o Comunicaciones:* Se tienen acceso a bases de datos de clientes prospectos y actuales (Email, nombre, teléfono, celular y dirección). Adicional desde el área de Comunicaciones tienen acceso a información de empleados (correo, nombre, email)
d. *Financiera:* información bancaria, nombre, cédula; así como información de empleados para el pago de la nómina.

La Gerencia de Bienestar y Entorno como Oficial de PDP (Protección de datos Personales) tiene el control de la información frente a las diferentes bases de datos personales que existen en la organización y será el responsable del registro de las mismas en el RNBD – Registro Nacional de Bases de Datos

Las nuevas bases de datos con información personal generadas a partir de nuevas negociaciones con clientes o proveedores o partir de ajustes a los procesos, debe reportarse de forma inmediata al Oficial de PDP y Líder de Riesgos y Control a través del formato “Bases de datos personales” por cada uno de los líderes de proceso.

Una vez identificada una base de datos con información personal, se cuenta con dos meses para ser reportada a la Superintendencia de Industria y Comercial, este reporte se realiza directamente por el Oficial de PDP

Posterior a este registro, cualquier cambio en la base de datos (finalidad, encargados, canales de atención, clasificación o tipos de datos, medidas de seguridad, política de protección de datos, transmisión y

transferencia de BD's) deberá reportarse mensualmente a la SIC los primeros 10 días hábiles del mes y a partir del 2018 anualmente entre el 2 de enero y 31 de marzo. Estas actualizaciones las podrán reportar desde el Site de Riesgos y Continuidad.

A la SIC, a través de la página http://www.sic.gov.co/drupal/registro-nacional-de-bases-de-datos, se informa el listado de las BD's mencionando la información personal que se solicita en estas, junto con su finalidad. Ver Manual de Ayuda en la misma dirección de la SIC.

3.2. Mediosde recolección de datos:

Los medios establecidos por APOLO GROUP S.A.S para la recepción de datos sensibles y/o personales están definidos de acuerdo a la finalidad del tratamiento.

Para información de clientes, se reciben a través de contacto directo entre el Ejecutivo comercial y el cliente, la cual se define mediante la firma de un contrato comercial, oferta mercantil u orden de compra. Para el registro del cliente debe existir autorización por parte del mismo para la consulta en centrales de riesgos y tratamiento de información sensible. **Ver Formato Vinculación de Clientes.**
La información de los titulares donde el cliente es el responsable del tratamiento, debe garantizarle a SISTEMAS APOLO S.A.S, que él cuenta con la autorización para que nuestra compañía pueda recolectar, usar, almacenar y circular o suprimir datos personales. En todos los contratos existe una cláusula para el manejo de datos personales y/o sensibles.

Para información de proveedores, se reciben a través de contacto directo entre el Líder del proveedor, área de Abastecimiento, la cual se define mediante la firma de un contrato comercial, oferta mercantil u orden de compra. Para el registro del proveedor debe existir autorización por parte del mismo para la consulta en centrales de riesgos y tratamiento de información personal. Ver **Formato Inscripción de Proveedores y Contratistas**.

El proveedor debe garantizar controles para la protección de bases de datos a las que pueda acceder de APOLO GROUP S.A.S o nuestros clientes y entregar a APOLO GROUP S.A.S. copia de su política de Protección de Datos Personales cuando sea necesario para el servicio que preste.

La información de candidatos y empleados activos o inactivos, es recolectada a través de Empresas Temporales, Head Hunters, Bolsas de Empleo, página web de la compañía, redes sociales o referenciadas. Se toma como autorización del tratamiento de datos sensibles el envío voluntario de su hoja de vida APOLO GROUP S.A.S. La autorización para los empleados queda registrada en el **formato Notificación Ley 1581 para Empleados.**

Para los UsuariosdePILA, la recolección se realiza a través del Aplicativo SOI, donde la persona natural o jurídica ingresa los datos y autoriza el uso de la información a través de esta plataforma aceptando los términos y condiciones.

La autorización puede constar en un documento físico, electrónico, en cualquier otro formato, y que dependerá del servicio, para garantizar su posterior consulta. Toda la información que haya sido capturada o almacenada en las bases de datos de APOLO GROUP S.A.S., se entiende que se hace a partir de la autorización del Titular. Si pasados **treinta (30) días hábiles**, contado a partir de la implementación de los mecanismos de comunicación, el Titular no ha contactado al Responsable o Encargado para solicitar la supresión de sus datos personales, el responsable y encargado podrán continuar realizando el Tratamiento de los datos contenidos en sus bases de datos para la finalidad o finalidades indicadas.

Con el procedimiento de autorización consentida se garantiza que se ha puesto en conocimiento del Titular de los datos personales, tanto el hecho que su información personal será recogida y utilizada para fines determinados y conocidos, como que tiene la opción de conocer cualquier alternación a los mismos y el uso específico que de ellos se ha dado. Lo anterior con el fin de que el Titular tome decisiones informadas con relación a sus datos personales y controle el uso de su información personal. La autorización es una declaración que informa al Titular de los datos personales y que contiene como mínimo:

- Quién recopila (responsable o encargado)
- Qué recopila (datos que se recaban)
- Para qué recoge los datos (las finalidades del tratamiento)
- Cómo ejercer derechos de acceso, corrección, actualización o supresión de los datos personales suministrados
- Si se recopilan datos sensibles
- Cada una de las áreas responsables del dato es responsable de custodiar las autorizaciones por parte del titular, es decir, el área de Abastecimiento conserva en la carpeta del proveedor su autorización, lo mismo ocurre para contratos con clientes y empleados, entre otros.

Antes de recolectar la información se debe dar aviso de privacidad al Titular sobre las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las características del tratamiento que se pretende dar a los datos personales.

Los datos personales que se encuentren en fuentes de acceso público, independientemente del medio por el cual se tenga acceso, entendiéndose aquellos datos o bases de datos que se encuentren a disposición del público como Facebook o Linkedin, pueden ser tratados por cualquier persona siempre y cuando, por su naturaleza, sean datos públicos.

APOLO GROUP S.A.S, podrá acceder a la información contenida en bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros para finalidades como: elemento de análisis para establecer y mantener una relación contractual, cualquiera que sea su naturaleza, así como para la evaluación de los riesgos derivados de una relación contractual vigente, elemento de análisis para hacer estudios de mercado o investigaciones comerciales o estadísticas, adelantamiento de cualquier trámite ante una autoridad pública o una persona privada, respecto del cual dicha información resulte pertinente y cualquier otra donde se haya obtenido autorización por parte del titular de la información

Excepciones**:** En los siguientes casos no será necesaria la autorización del Titular:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública. Esto incluye: 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.
- 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.

Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley

Nota: La administración de datos semiprivados y privados requiere el consentimiento previo y expreso del titular de los datos, salvo en el caso del dato financiero, crediticio, comercial, de servicios y el proveniente de terceros países el cual no requiere autorización del titular. En todo caso, la administración de datos semiprivados y privados se sujeta al cumplimiento de los principios de la administración de datos personales

4. ALMACENAMIENTO:

Las autorizaciones serán almacenadas según las definiciones entregadas por los Responsables de las Bases de datos y serán garantes de definir los accesos y controles para garantizar la seguridad de la información.

La información de empleados es administrada por el área de Gestión Humana y es almacenada en las hojas de vida de los empleados que se encuentra en el Archivo Corporativo, unidad de red del área y aplicativos para la administración de nómina y hojas de vida

Las Bases de datos de clientes es administrada por cada una de las zonas y tienen acceso el área de Fidelización y Servicios, Comercial, Comunicaciones Integradas y Mercadeo. Estas Bases de datos son almacenadas en el CRM, ERP y unidades de red.

Las copias de seguridad que se hacen a las compañías, las cuales comprenden sus aplicativos ERP, servidor de archivos e información general se respalda en forma cifrada con un algoritmo AES-256 (clave privada). Seguridad mejorada con la encriptación SSL de 128 bits en las transferencias, encriptación AES de 256 bits en el almacenamiento con una tecla definida por el usuario que no se guarda en ningún lugar en los servidores.

La información se es almacena en servidores de alto rendimiento, los cuales disponen de seguridad, ambiente autónoma, sistema antiincendios, canal de fibra dedicado los cuales tienen servicio garantizado con SLA del 99,9. NODO SV4 CALIFONIA POR PLATAFORMA 500GIGAS.COM

Nuestros servidores de almacenamiento están rigurosamente protegidos pasando por 3 firewalls (firewall proveído por el centro de datos, firewall global de Linux y firewall configurado en cada servidor de datos).

La información de proveedores es administrada por el área de Abastecimiento y almacenada a través del ERP y unidad de red compartida.

Las bases de datos de la operación es administrada por cada líder de servicio/contrato y área de Infraestructura Interna. Esta es almacenada en los Datacenter principales de APOLO GROUP S.A.S. La documentación física como contratos con terceras partes, es almacenada en el Archivo Corporativo, donde el acceso y el tiempo de conservación es definido por cada líder de proceso y está documentado en el proceso de Administración Documental, liderado por el área de Servicios internos de donde se garantiza, los lineamientos para el tratamiento, conservación y supresión de la información.

APOLO GROUP S.A.S, actuando como Responsable y/o Encargado del Tratamiento sólo puede recolectar, almacenar, usar o circular los datos personales durante el tiempo que sea razonable y necesario, de acuerdo con las finalidades que justificaron el tratamiento, atendiendo a las disposiciones aplicables a la materia de que se trate y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información. Una vez cumplida la o las finalidades del tratamiento y sin perjuicio de normas legales que dispongan lo contrario, se procede a la supresión de los datos personales a los que haya tenido acceso. Todo lo anterior respectando el cumplimiento de requisitos legales y contractuales, es decir que si hay una obligación legal de conservar la información, no se puede eliminar, esto prevalece frente a la solicitud del titular de eliminar sus datos.

En cuanto a los otros registros de los procesos, por cada uno se define el responsable de su custodia, tiempo de conservación y disposición final.

5. USO Y CIRCULACIÓN:

De acuerdo a lo establecido por la compañía, el uso y tratamiento de los datos personales están enmarcados según el propósito definido para el servicio que se preste, de acuerdo a las políticas de seguridad definida por la compañía.

Dentro de los controles de seguridad se tiene como alcance:

Todo el personal de la Organización se encuentra comprometido con la seguridad de la información, garantizando su protección y uso adecuado mediante el cumplimiento de las políticas y directrices definidas y la implementación del Manual y guías de Seguridad en cada uno de sus anexos; así mismo frente a la protección de los activos de información que le son asignados bajo su responsabilidad.

Por otro lado, el personal de la Compañía implementa los controles respectivos para evitar el acceso, destrucción y divulgación de información no autorizada, evitando cualquier tipo de perjuicios contra el negocio, sus empleados, sus clientes, sus socios de negocios o cualquier entidad o parte interesada con una afiliación comercial.

Cada líder de proceso es responsable de garantizar la implementación del Manual de Seguridad con su grupo de colaboradores, realizar seguimiento y establecer los correctivos que sean necesarios para preservar la seguridad de los activos de información asignados.

El nivel de protección de los activos de información de la Compañía depende de su clasificación en la Guía de Manejo de Activos (confidencial, privado, personal, sensible, restringido, interno o público).

La información que se procesa, maneja y transmite por medios electrónicos o físicos debe adecuarse a los modelos de seguridad definidos para la misma.

El Plan de **Continuidad de Negocio** es implementado, monitoreado y analizado permanentemente por parte del Comité de Administración de Crisis (CAC) o en su defecto el Comité de Continuidad (CC).

Cada Líder de Recuperación de Negocio es responsable de mantener actualizados los procedimientos alternos de operación y de informar oportunamente al área de Riesgos y Control sobre el cambio o modificación de algún procedimiento alterno de continuidad, para que estos se hagan de manera oficial y sean comunicados al personal respectivo.

El Director de Continuidad de Negocio en su rol, es responsable por mantener la coordinación en la actualización de los procedimientos alternos de recuperación y las estrategias de continuidad con relación al direccionamiento estratégico de la Compañía, así como de garantizar la ejecución, seguimiento, evaluación y mejoramiento de las pruebas del plan.

Todos los empleados y proveedores son responsables de informar a su líder directo o al responsable del proceso respectivo los **eventos o incidentes de seguridad** que se presenten (ya sean de seguridad física o lógica), para establecer las acciones necesarias que disminuyan la probabilidad de ocurrencia de los mismos en los procesos críticos del negocio. La forma de proceder en estos casos, se encuentra descrita en las Guías de “Administración de Incidentes de Seguridad Lógica” y “Seguridad Física”, fin para el cual se cuenta con la herramienta de Gestión de Incidentes.

Con el objetivo de impedir el acceso no autorizado a la información, la compañía cuenta con el procedimiento para la **Gestión de Accesos lógicos**, con el objetivo de implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización, controlando la seguridad en la conexión entre la red de la compañía y otras redes públicas o privadas, impidiendo el acceso no autorizado a los sistemas de información y plataforma tecnológica y garantizando la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

Todos los empleados de la Compañía que laboren en instalaciones de terceros (clientes) se acogerán a las políticas definidas, planes de emergencia, planes de continuidad y temas relacionados con salud ocupacional que estén establecidos en dichas instalaciones, según lo descrito en la guía Gestión de la Continuidad de Negocio.

Los proveedores/contratistas o asesores son responsables de implementar los controles de seguridad definidos, garantizando la confidencialidad, integridad y disponibilidad de la información y activos de información que le sean asignados. Por lo tanto es responsabilidad del líder, al interior de APOLO GROUP S.A.S, de dicho contrato, garantizar la divulgación de esta información y validar la aplicación de estas políticas por los terceros a su cargo.

Para el control de la **Seguridad de los Recursos humanos** al interior de la organización, la compañía ha implementado diferentes controles y ha asignado responsabilidades que aseguran el trabajo bajo los términos y condiciones de seguridad requeridos por el Negocio, dentro de estos se cuenta verificación de antecedentes laborales de los empleados para conocer el comportamiento del candidato en el entorno laboral, se tiene estipulado un apartado dentro de la descripción de cargos y perfil relacionado al cumplimiento en la seguridad de la información a la que pueda acceder y esto es un compromiso que se realiza a través de la firma del contrato laboral con nuestra compañía y una vez terminada la relación, se asegura la devolución de los activos de información que dicha persona tenía a su disposición para las labores propias del cargo, así como el retiro de acceso.

Respaldo de información: La compañía determina los requerimientos para resguardar cada software o dato en función de su criticidad, controlando y ejecutando la realización de salvaguardado, así como la prueba periódica de su restauración. Los sistemas de resguardo son probados periódicamente, asegurando que cumplen con los requerimientos de los planes de continuidad de las actividades de la organización

Se cuenta con lineamientos para **la adquisición y el mantenimiento de sistemas de información** que garanticen que la seguridad sea una parte integral de los mismos, previniendo errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones, protegiendo la confidencialidad, autenticidad e integridad a través de medios criptográficos antes, durante y después de la prestación del servicio.

La compañía define lineamiento frente a la **seguridad física y ambiental** brindando el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones de la organización. Asimismo, pretende mitigar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad o controles de acceso, facilitando la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible de la organización, de accesos físicos no autorizados.

Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio, los cuales en ningún caso podrán ser inferiores a los que ley de protección de datos personales exige a sus destinatarios. Esta prohibición no regirá cuando se trate de:

- Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.
- Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública.
- Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable,
- Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad .
- Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.

- Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- Las transmisiones internacionales de datos personales que se efectúen entre un Responsable y un Encargado para permitir que el encargado realice el tratamiento por cuenta del responsable, no requerirán ser informadas al Titular ni contar con su consentimiento cuando exista un contrato que garantice: dar Tratamiento, a nombre del Responsable, a los datos personales conforme a los principios que los tutelan, salvaguardar la seguridad de las bases de datos en los que se contengan datos personales y guardar confidencialidad respecto del tratamiento de los datos personales

Como control adicional, APOLO GROUP S.A.S realiza el reporte máximo dos meses después de creada una base de datos personal a la Superintendencia de Industria y Comercio, para que pueda ser consultado por cualquier ciudadano

La compañía podrá hacer uso de las BD para todo tipo de acciones que se requieran para análisis interno de la información, como son fines estadísticos o de control, siempre y cuando no vaya en contravía de los derechos del titular del dato.

5.1. *Transporte, desecho o reutilizado de documentos:*

En el servicio de Gestión de Información, para el transporte de documentos con información personal y/o confidencial, se garantizar el manejo de tulas con precinto cerrado. Para los documentos que son copias o no se requieren para el procesamiento, se cuenta con destructoras de papel en los Centros de Operaciones y/o el Auxiliar de Producción debe rasgarlos.

Para los documentos como correspondencia, información financiera, entre otros, se garantiza que su circularización se realiza en sobre cerrado.

Los documentos que son reciclados y que tengan información confidencial, se debe garantizar rasgarlos antes de depositarlos en la basura.

No se reutilizan documentos con información confidencial o personal.

6. CONSULTA

Los únicos que podrán acceder a la información que reúna las condiciones establecidas por ley son los siguientes:

a) A los Titulares, sus causahabientes o sus representantes legales.
b) A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.
c) A los terceros autorizados por el Titular o por la ley.
d) A otros operadores de datos, cuando se cuente con autorización del titular, o cuando sin ser necesaria la autorización del titular el banco de datos de destino tenga la misma finalidad o una finalidad que comprenda la que tiene el operador que entrega los datos. Si el receptor de la información fuere un banco de datos extranjero, la entrega sin autorización del titular sólo podrá realizarse dejando constancia escrita de la entrega de la información y previa verificación por parte del operador de que las leyes del país respectivo o el receptor otorgan garantías suficientes para la protección de los derechos del titular.

Las consultas se podrán realizar a través de los siguientes medios:

Empleados, clientes y proveedores a través de la página web por contáctenos, correo corporativo.

Adicional, para proveedores puede solicitar la información directamente al área de Abastecimiento, o para clientes, pueden solicitar su información directamente al ejecutivo de cuenta info@sistemasapolo.com.
Para empleados puede consultar sus datos en los aplicativos NOMINAI y Hojas de vida o solicitarlos a través de la herramienta de gestión interna al área de Gestión Humana.
Para APOLO GROUP S.A.S los aportantes pueden acceder a su información a través de la línea telefónica de Planilla Asistida.
Las entidades públicas, administrativas o entes de vigilancia y control podrán solicitar la información a través de comunicado directo al Gerente General o Gerente de Bienestar y Entorno.

Cada área responsable de la base de datos debe registrar los casos generados por los Titulares en el formulario dispuesto en la Intranet de la compañía y generar su solución de forma oportuna. Para los casos que llegan por Contáctenos es responsabilidad del área de Fidelización y Servicio realizar el escalamiento correspondiente al área responsable. El Líder de Riesgos y Control realiza seguimiento mensual al comportamiento de estos casos.

Nota:
La consulta será atendida en un término máximo de **diez (10) días hábiles** contados a partir de la fecha de recibo de la misma. Cuando no sea posible atender la consulta dentro de dicho tiempo, se debe informar al interesado los motivos de la demora y notificar 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.

7. RECLAMOS

El Titular o quién este designe, que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento frente a la protección de sus datos, podrán presentar un reclamo ante APOLO GROUP S.A.S como Responsable o Encargado del tratamiento de su información, el cual será tramitado bajo las siguientes reglas:

i. El reclamo se formula mediante solicitud dirigida a APOLO GROUP S.A.S a través de los medios definidos en el ítem de Consulta, indicando el nombre completo, número de identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y anexando los documentos que lo soporta, en caso de requerirse. Si el reclamo resulta incompleto, se requerirá al interesado dentro de **los cinco (5) días siguientes** a la recepción del reclamo para que aclare o entregue la información faltante. 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 recibidos los reclamos completos se ingresarán a Formulario en un tiempo no mayor a **dos (2) días hábiles**, indicando el estado "En trámite" y el motivo del mismo. En éste formulario se registrará la información solicitada de acuerdo al tipo de reclamo definido por la Ley 1581.

En caso de quién reciba el reclamo no sea la persona competente para gestionarlo y dar respuesta, es su responsabilidad trasladarlo, en la medida de sus posibilidades, a quien corresponda en un término máximo de **dos (2) días hábiles**, e informa de la situación al interesado.

Si por alguna circunstancia se recibe un reclamo que en realidad no debería ir dirigido para APOLO GROUP S.A.S, éste dará respuesta al solicitante indicando la situación, máximo **en dos (2) días hábiles**.

ii. El término máximo para atender el reclamo es de quince **(15) días hábiles** contados a partir del día siguiente a la fecha de su recibo. Para los casos en que no sea posible atenderlo en este tiempo, se informará al interesado antes de su vencimiento 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.

iii. El Titular puede escalar el reclamo a la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante APOLO GROUP S.A.S

Los reclamos sobre los datos personales que realiza el titular (dueño del dato) también deben ser reportados a la SIC máximo los primeros **15 días hábiles de cada mes** a partir del reporte de la base de datos.

7.1. Supresión:

Los Titulares podrán en cualquier momento solicitar a APOLO GROUP S.A.S la supresión de sus datos personales y/o revocar la autorización otorgada para el Tratamiento de los mismos, mediante la presentación de un reclamo o contacto por los mismos medios establecidos en el ítem de Consulta.

La solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el Titular tenga un deber legal o contractual de permanecer en la base de datos, es decir que si hay una obligación legal de conservar la información, no se puede eliminar. Esto prevalece frente a la solicitud del titular de eliminar sus datos.

Si vencido el término legal respectivo, APOLO GROUP S.A.S actuando en calidad de Encargados o Responsables del tratamiento, según fuera el caso, no eliminan los datos personales, el Titular tendrá derecho a solicitar a la Superintendencia de Industria y Comercio que ordene la revocatoria de la autorización y/o la supresión de los datos personales.

8. MONITOREO Y CONTROL

La compañía cuenta con un modelo de gestión de riesgos, el cual según la criticidad de la información, valoran los riesgos a los que se pueda ver expuesta de acuerdo a su probabilidad e impacto. Para esto se realiza una identificación y monitoreo permanente a los que se pueda ver expuesta cada una de las partes de la compañía, con el objetivo de definir planes de trabajo para disminuir su valor.

Adicional, según el modelo interno de la compañía, cada uno de los procesos establecidos y líderes de los mismos, garantizar su correcta implementación y cumplimiento. Así mismo el rol de Oficial de Registro de Bases de datos realiza el monitoreo de las bases de datos personales y eficacia de los controles implementados para garantizar su seguridad.

Como parte de Auditoría Interna, se verifica el cumplimiento de los controles para garantizar la seguridad de los datos personales.