13 de julio de 2011
PJD-07-2011

Señor
Oldemar Castro, Director
Departamento de Tecnologías de Información

Estimado señor:

En atención a su solicitud de realizar un análisis jurídico sobre legalidad de tener la información de la Superintendencia de Pensiones (SUPEN) en Servidores en la Nube, esta División Jurídica emite el siguiente **criterio legal**.

I. Antecedentes.

En consulta planteada por el Departamento de Tecnologías de Información se solicita a esta Asesoría Jurídica analizar la legalidad de tener la información de la Superintendencia de Pensiones (SUPEN) en Servidores en la Nube.

Mediante anotación en el Sistema de Trámites, realizada el 25 de abril, el Encargado del Proceso de Tecnologías de Información aclaró lo siguiente:

> *"Se va a efectuar el traslado de la información de el Sistema de VES y la página WEB".*
>
> *El VES tiene la siguiente información Transferencia de Información (Inversiones, Afiliados y Saldos Contables)*
> *Documentación*
> *Proceso de Inversiones*
> *Consultas*
> *Incentivos Fiscales*
> *Información Cualitativa*
> *Actas Electrónicas*
> *SVaR*
> *Compensación Electrónica*
>
> *La información que va a estar en la nube, va a ser solamente la Base de Datos de SQL Server, ya que no se puede pasar la información de la Base de Datos de ORACLE. Esto puede ser temporal, porque hay otro proyecto para pasar la información de la base de datos de ORACLE a la base de datos SQL Server".*

II. Sobre la computación en la Nube

Debido a lo novedoso de la temática sometida a consulta, es necesario tener presente lo que implica la computación en la nube o "*Cloud computing".* Al

respecto, en la página web: ***http://es.wikipedia.org/wiki/Computación_en_nube***[1], se indica que según la IEEE Computer Society, la computación en la nube es un *"… paradigma en el que la información se almacena de manera permanente en servidores de Internet y se envía a cachés temporales de cliente, lo que incluye equipos de escritorio, centros de ocio, portátiles, etc".*

La citada publicación señala que existen los siguientes tipos de nubes:

- *"Las nubes públicas se manejan por terceras partes, y los trabajos de muchos clientes diferentes pueden estar mezclados en los servidores, los sistemas de almacenamiento y otras infraestructuras de la nube. Los usuarios finales no conocen qué trabajos de otros clientes pueden estar corriendo en el mismo servidor, red, discos como los suyos propios.*
- *Las nubes privadas son una buena opción para las compañías que necesitan alta protección de datos y ediciones a nivel de servicio. Las nubes privadas están en una infraestructura en-demanda manejada por un solo cliente que controla qué aplicaciones debe correr y dónde. Son propietarios del servidor, red, y disco y pueden decidir qué usuarios están autorizados a utilizar la infraestructura.*
- *Las nubes híbridas combinan los modelos de nubes públicas y privadas. Usted es propietario de unas partes y comparte otras, aunque de una manera controlada. Las nubes híbridas ofrecen la promesa del escalado aprovisionada externamente, en-demanda, pero añaden la complejidad de determinar cómo distribuir las aplicaciones a través de estos ambientes diferentes. Las empresas pueden sentir cierta atracción por la promesa de una nube híbrida, pero esta opción, al menos inicialmente, estará probablemente reservada a aplicaciones simples sin condicionantes, que no requieran de ninguna sincronización o necesiten bases de datos complejas."*

En cuanto a los beneficios de la computación en la nube, esta publicación destaca los siguientes:

"Beneficios:

- *Integración probada de servicios Red. Por su naturaleza, la tecnología de Cloud Computing se puede integrar con mucha mayor facilidad y rapidez con el resto de sus aplicaciones empresariales (tanto software tradicional como Cloud Computing basado en infraestructuras), ya sean desarrolladas de manera interna o externa.*

- *Prestación de servicios a nivel mundial. Las infraestructuras de Cloud Computing proporcionan mayor capacidad de adaptación, recuperación de desastres completa y reducción al mínimo de los tiempos de inactividad.*

- *Una infraestructura 100% de Cloud Computing no necesita instalar ningún tipo de hardware. La belleza de la tecnología de Cloud Computing es su simplicidad y el hecho de que requiera mucha menor inversión para empezar a trabajar.*

- *Implementación más rápida y con menos riesgos. Podrá empezar a trabajar muy rápidamente gracias a una infraestructura de Cloud Computing. No tendrá que volver a esperar meses o años e invertir grandes cantidades de dinero antes de que un usuario inicie sesión en su nueva solución. Sus aplicaciones en tecnología de Cloud Computing estarán disponibles en cuestión de semanas o meses, incluso con un nivel considerable de personalización o integración.*

[1] Según consulta realizada el 12 de julio de 2011.

- *Actualizaciones automáticas que no afectan negativamente a los recursos de TI. Si actualizamos a la última versión de la aplicación, nos veremos obligados a dedicar tiempo y recursos (que no tenemos) a volver a crear nuestras personalizaciones e integraciones. La tecnología de Cloud Computing no le obliga a decidir entre actualizar y conservar su trabajo, porque esas personalizaciones e integraciones se conservan automáticamente durante la actualización.*

- *Contribuye al uso eficiente de la energía. En este caso, a la energía requerida para el funcionamiento de la infraestructura. En los datacenters tradicionales, los servidores consumen mucha más energía de la requerida realmente. En cambio, en las nubes, la energía consumida es sólo la necesaria, reduciendo notablemente el desperdicio."*

En cuanto a las desventajas, la misma publicación señala las siguientes:

"Desventajas:

- *La centralización de las aplicaciones y el almacenamiento de los datos origina una dependencia de los proveedores de servicios.*

- *La disponibilidad de las aplicaciones están atadas a la disponibilidad de acceso a internet.*

- ***Los datos "sensibles" del negocio no residen en las instalaciones de las empresas por lo que podría generar un contexto de alta vulnerabilidad para la sustracción o robo de información.***

- *La confiabilidad de los servicios depende de la 'salud' tecnológica y financiera de los proveedores de servicios en nube. Empresas emergentes o alianzas entre empresas podrían crear un ambiente propicio para el monopolio y el crecimiento exagerado en los servicios.*

- *La disponibilidad de servicios altamente especializados podría tardar meses o incluso años para que sean factibles de ser desplegados en la red.*

- *La madurez funcional de las aplicaciones hace que continuamente estén modificando sus interfaces por lo cual la curva de aprendizaje en empresas de orientación no tecnológica tenga unas pendientes pequeñas.*

1. ***Seguridad. La información de la empresa debe recorrer diferentes nodos para llegar a su destino, cada uno de ellos (y sus canales) son un foco de inseguridad. Si se utilizan protocolos seguros, HTTPS por ejemplo, la velocidad total disminuye debido a la sobrecarga que requieren estos protocolos.***

- *Escalabilidad a largo plazo. A medida que más usuarios empiecen a compartir la infraestructura de la nube, la sobrecarga en los servidores de los proveedores aumentará, si la empresa no posee un esquema de crecimiento óptimo puede llevar a degradaciones en el servicio o jitter altos."* El destacado no es del original.

III. Sobre la información contenida en el VES y en la página WEB de la SUPEN.

La Ventanilla Electrónica de Servicios (VES) y la página web de la Superintendencia de Pensiones se ejecutan actualmente en servidores localizados en esta Superintendencia.

En el VES consta la siguiente información:

- Transferencia de Información (Inversiones, Afiliados y Saldos Contables)
- Documentación
- Proceso de Inversiones
- Consultas
- Incentivos Fiscales
- Información Cualitativa
- Actas Electrónicas
- SVaR
- Compensación Electrónica

Como se puede observar, consta en este sistema información relacionada con datos personales de los afiliados, así como con el proceso de inversiones que realizan las entidades reguladas por la SUPEN.

En cuanto a la página web, a través del sitio en Internet http://www.supen.fi.cr, la Superintendencia ofrece su portal de información al público en general, por lo que en este portal no consta información relacionada con datos personales de los afiliados ni otra que deba considerarse de carácter confidencial.

Existe un proyecto denominado "Sistemas en la Nube", que tiene como objetivo el traslado de estos dos sistemas a servidores en la Nube de Microsoft. El presente criterio fue solicitado con el fin de determinar la viabilidad legal de realizar este traslado, considerando que, particularmente en el caso del VES, en este sistema consta información relacionada con datos personales de los afiliados y otra relacionada con el proceso de inversiones.

IV. Marco normativo.

En vista de lo anterior, para atender la consulta planteada por el Departamento de Tecnologías de Información se debe tener en consideración el siguiente marco normativo:

a) Normativa constitucional

En relación con el derecho a la intimidad, a la libertad y al secreto de las comunicaciones resulta relevante el artículo 24 de la Constitución Política, cuyo texto dispone:

> **"Artículo 24.-**
> *"Se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones.*

Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier tipo de los habitantes de la República. Sin embargo, la ley, cuya aprobación y reforma requerirá los votos de dos tercios de los diputados de la Asamblea Legislativa, fijará en qué casos podrán los Tribunales de Justicia ordenar el secuestro, registro o examen de los documentos privados, cuando sea absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento.

Igualmente, la Ley determinará en cuáles casos podrán los Tribunales de Justicia ordenar que se intervenga cualquier tipo de comunicación e indicará los delitos en cuya investigación podrá autorizarse el uso de esta potestad excepcional y durante cuánto tiempo.

Asimismo, señalará las responsabilidades y sanciones en que incurrirán los funcionarios que apliquen ilegalmente esta excepción. Las resoluciones judiciales amparadas a esta norma deberán ser razonadas y podrán ejecutarse de inmediato. Su aplicación y control serán responsabilidad indelegable de la autoridad judicial.

La ley fijará los casos en que los funcionarios competentes del Ministerio de Hacienda y de la Contraloría General de la República podrán revisar los libros de contabilidad y sus anexos para fines tributarios y para fiscalizar la correcta utilización de los fondos públicos.

Una ley especial, aprobada por dos tercios del total de los diputados, determinará cuáles otros órganos de la Administración Pública podrán revisar los documentos que esa ley señale en relación con el cumplimiento de sus competencias de regulación y vigilancia para conseguir fines públicos. Asimismo, indicará en qué casos procede esa revisión.

No producirán efectos legales, la correspondencia que fuere sustraída ni la información obtenida como resultado de la intervención ilegal de cualquier comunicación."

En relación con esta norma, en la OJ-103-2010 la Procuraduría General de la República señaló lo siguiente:

"... I- LA AUTODETERMINACION INFORMATIVA: UN DERECHO FUNDAMENTAL

El artículo 24 de la Constitución Política es el fundamento de diversos derechos fundamentales que regulan el derecho a la intimidad y a la vida privada. *En efecto, este artículo consagra los derechos fundamentales a la intimidad, a la inviolabilidad de los documentos privados, el secreto de las comunicaciones* ***y el derecho a la autodeterminación informativa o derecho a tener control sobre las informaciones que terceros ostenten sobre la persona de que se trate.*** *Estos derechos tienen como fundamento la dignidad de la persona y su ejercicio supone la autodeterminación consciente y responsable de la propia vida. La dignidad es inherente al ser humano, y es el mínimo jurídico que se le debe asegurar a la persona con el objeto de que se respete su condición de tal y un mínimo de calidad de vida humana.* ***En el respeto de los derechos derivados del artículo 24 se manifiesta el respeto a la dignidad humana.*** (El subrayado no es del original).

b) Decreto Legislativo N° 8968, Ley de protección de la persona frente al tratamiento de sus datos personales

Se encuentra aprobado por la Asamblea Legislativa, y pendiente de sanción y publicación por parte del Poder Ejecutivo, el decreto legislativo N° 8968, Ley de protección de la persona frente al tratamiento de sus datos personales.

Se trata de una ley de orden público que tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa[2] en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes (artículos 1).

De acuerdo con el artículo 2, esta Ley será de aplicación a los datos personales que figuren en bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos.

De interés para este criterio resultan las siguientes definiciones contenidas en el artículo 3:

- Base de datos: cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales, que sean objeto de tratamiento o procesamiento, automatizado o manuales, cualquiera que sea la modalidad de su elaboración, organización o acceso.
- Datos personales: cualquier dato relativo a una persona física identificada o identificable[3].
- Datos personales de acceso irrestricto: los contenidos en bases de datos públicas de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados.
- Datos personales de acceso restringido: los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública.

---

[2] En este sentido, en la OJ-103-2010 la Procuraduría ha señalado que:
"El derecho de autodeterminación informática otorga protección a los datos personales que hayan sido recolectados, registrados o tratados en ficheros, archivos, registros o bases de datos, sean estos públicos o privados. Este derecho tiene como núcleo fundamental de protección la persona humana, a la cual se le reconoce un derecho de autodeterminación, que se manifiesta en el derecho a saber quién tiene información sobre ella, qué clase de información se tiene y con qué motivo la misma ha sido recabada. Un derecho que permite a la persona ejercer control sobre la información personal que le concierne, contenida tanto en registros públicos como privados. Se trata de evitar que a través del conocimiento que de esos registros tengan, la Administración o los particulares puedan ejercer un control sobre el individuo. Un control que resulta absolutamente contrario a la dignidad humana.

[3] Como complemento puede tenerse en consideración lo señalado por la Procuraduría General de la República en la OJ-103-2010, en el sentido que: *"Se entiende por **datos personales** los que correspondan a una persona identificada o identificable: datos relativos al nacimiento, fallecimiento, estado civil, número de identificación, domicilio, enfermedades, profesión, patrimonio, afiliación política, sexo, raza, creencias políticas o religiosas. El concepto de dato personal está referido a la posibilidad de identificación del titular de esos datos, por lo que bien cubre datos que sean de fácil conocimiento público, como son el sexo o el color de la piel, los cuales incluso son susceptibles de una protección mayor, en tanto como datos sensibles su conocimiento y uso puede dar lugar a discriminaciones".* El subrayado no es del original.

- Datos sensibles: información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros.
- Deber de confidencialidad: obligación de los responsables de bases de datos, personal a su cargo y del personal de la Agencia de Protección de Datos de los Habitantes (Prodhab), de guardar la confidencialidad con ocasión del ejercicio de las facultades dadas por esta ley, principalmente cuando se acceda a información sobre datos personales y sensibles. Esta obligación perdurará aun después de finalizada la relación con la base de datos.
- Interesado: persona física, titular de los datos que sean objeto del tratamiento automatizado o manual.
- Responsable de la base de datos: persona física o jurídica que administre, gerencie o se encargue de la base de datos, ya sea esta una entidad pública o privada, competente, con arreglo a la ley, para decidir cuál es la finalidad de la base de datos, cuáles categorías de datos de carácter personal deberán registrase y qué tipo de tratamiento se les aplicarán.
- Tratamiento de datos personales: cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros.

Se reconoce el derecho de toda persona a la autodeterminación informativa, la cual abarca el conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales. A esta se le da también el carácter de derecho fundamental, con el objeto de controlar el flujo de informaciones que conciernen a cada persona, derivado del derecho a la privacidad (artículo 4).

De interés para este criterio, en el artículo 9 se establece el tratamiento de los datos personales de acceso restringido y de los de acceso irrestricto. Los primeros son los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública. Su tratamiento será permitido únicamente para fines públicos o si se cuenta con el consentimiento expreso del titular.

Los segundos son aquellos contenidos en bases de datos públicas de acceso general, según lo dispongan las leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados. No se considerarán contemplados en esta última categoría: la dirección exacta de la residencia, excepto si su uso es producto de un mandato, citación o notificación administrativa o judicial, o bien, de una operación bancaria o financiera, la fotografía, los números de teléfono privados y otros de igual naturaleza cuyo tratamiento pueda afectar los derechos y los intereses de la persona titular.

Cuando se soliciten datos de carácter personal, el decreto prevé que será necesario informar de previo a las personas titulares o a sus representantes, de modo expreso, preciso e inequívoco, entre otros:

- De la existencia de una base de datos de carácter personal.
- De los fines que se persiguen con la recolección de estos datos.
- De los destinatarios de la información, así como de quiénes podrán consultarla.
- Del tratamiento que se dará a los datos solicitados.
- De la identidad y dirección del responsable de la base de datos.

En cuanto al responsable de la base de datos, el artículo 10 establece que este deberá adoptar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a esta ley.

Dichas medidas deberán incluir, al menos, los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual, para garantizar la protección de la información almacenada. Se prohíbe registrar datos personales en bases de datos que no reúnan las condiciones que garanticen plenamente su seguridad e integridad, así como la de los centros de tratamiento, equipos, sistemas y programas. Se establece que por vía de reglamento se establecerán los requisitos y las condiciones que deban reunir las bases de datos automatizadas y manuales, y de las personas que intervengan en el acopio, almacenamiento y uso de los datos (a la fecha este reglamento no se encuentra promulgado).

El decreto establece la obligación de la persona responsable y quienes intervengan en cualquier fase del tratamiento de datos personales de guardar el secreto profesional o funcional, aun después de finalizada su relación con la base de datos. Estos solo podrán transferir datos contenidos en esas bases cuando el titular del derecho haya autorizado expresa y válidamente tal transferencia y se haga sin vulnerar los principios y derechos reconocidos en esta ley.

De acuerdo con el artículo 12, las personas físicas y jurídicas, públicas y privadas, que tengan entre sus funciones la recolección, el almacenamiento y el uso de datos personales, podrán emitir un protocolo de actuación en el cual establecerán los pasos que deberán seguir en la recolección, el almacenamiento y el manejo de los datos personales, de conformidad con las reglas previstas en el Decreto.

Para que sean válidos, los protocolos de actuación deberán ser inscritos, así como sus posteriores modificaciones, ante la Agencia de Protección de Datos de los habitantes (Prodhab)[4]. La Prodhab podrá verificar, en cualquier momento, que la base de datos esté cumpliendo cabalmente con los términos de su protocolo. Es importante tener en cuenta que la manipulación de datos con base en un protocolo de actuación inscrito ante la Prodhab hará presumir, "iuris tantum", el

[4] Órgano de desconcentración máxima adscrito al Ministerio de Justicia y Paz que se crea en este Decreto Legislativo.

cumplimiento de las disposiciones contenidas en esa ley, para los efectos de autorizar la cesión de los datos contenidos en una base.

c) Normativa de SUPEN sobre confidencialidad de la información

En relación con la normativa que rige a la Superintendencia de Pensiones es necesario considerar las siguientes disposiciones:

- El artículo 67 de la Ley de Protección al Trabajador, según el cual:

  "ARTÍCULO 67. Confidencialidad de la información
  Deberán guardar estricta confidencialidad respecto de esa información las autoridades, los apoderados, gerentes, administradores y cualquier persona que, en razón de su labor en un ente regulado, ***acceda a información de las inversiones de los recursos de un fondo que aún no haya sido divulgada oficialmente en el mercado*** *y que, por su naturaleza, sea capaz de influir en las cotizaciones de los valores de dichas inversiones. Quienes actúen en contravención de lo señalado, a solicitud de la Superintendencia, deberán ser destituidos, mediante la aplicación de la legislación laboral correspondiente; sin perjuicio de las sanciones penales que puedan aplicarse.*
  Asimismo, se prohíbe a las personas mencionadas valerse, directa o indirectamente, de la información reservada con el fin de obtener, para sí o para otros, de los fondos administrados, ventajas mediante la compra o venta de valores.
  Ninguna ***información registrada en las cuentas individuales*** *podrá ser suministrada a terceros, excepto en los casos previstos en esta Ley."* El resaltado no es del original.

  En relación con este artículo, mediante SP-A-028 del 08 de julio del 2003, se dispuso:

  "…6- Que en aras de preservar el principio de confidencialidad de la información estatuido en artículo 67 de la Ley 7983, la Superintendencia pondrá a disposición de las entidades autorizadas, únicamente aquella información que resulte indispensable para identificar correctamente los afiliados a los que corresponden los registros erróneos, según los indicios que la Operadora disponga en su base de datos de afiliados…"

- El artículo 53 de la Ley del Régimen Privado de Pensiones Complementarias y Reformas a la Reguladora del Mercado de Valores y Código de Comercio, N°7523, que establece:

  "Artículo 53.- Faltas contra la confidencialidad
  Quienes contravengan las prohibiciones citadas en el artículo 67 de la Ley de Protección al Trabajador serán sancionadas con multa de uno a seis salarios base, que aplicará la Superintendencia en beneficio del propio fondo y con cargo a la operadora respectiva. Por salario base se entenderá el definido en la ley no."

De la normativa transcrita se extrae que existe un deber de confidencialidad respecto de la información de las inversiones de los recursos de un fondo que aún no haya sido divulgada oficialmente en el mercado y que, por su naturaleza, sea capaz de influir en las cotizaciones de los valores de dichas inversiones. De igual manera, de conformidad con el artículo 67 de la LPT mencionado, ninguna información registrada en las cuentas individuales podrá ser suministrada a terceros, excepto en los casos previstos en esta Ley.

d) Otra normativa vigente relacionada con Derecho Informático.

En el documento adjunto se detalla la normativa en materia de Derecho Informático que actualmente se encuentra vigente.

Índice de normativa.docx

De una revisión detallada de cada una de las disposiciones señaladas en el referido documento, se concluye que no existe ninguna norma que regule el tema de computación en la nube.

V. Análisis de fondo

En relación con la consulta planteada por el Departamento de Tecnologías de Información, esta Asesoría valoró la legislación vigente en materia de Derecho Informático y no encontró ninguna norma que regule de manera específica la transferencia de sistemas a la Nube.

No obstante, considerando que la información que consta en los sistemas a trasladar, en particular en el VES, se encuentra relacionada con el manejo de datos personales de los afiliados, es necesario tener presente en este análisis la normativa vigente en materia de protección de este tipo de datos, y en general, la que se encuentra relacionada con el deber de confidencialidad establecido en el artículo 67 de la Ley de Protección al Trabajador.

En este sentido, considera esta Asesoría que en materia de tratamiento de datos personales de los afiliados, así como otro tipo de información que de acuerdo con el artículo 67 de la LPT tenga carácter confidencial, la SUPEN, y en particular los responsables del manejo de las bases de datos, están obligados a tomar todas las medidas de índole técnica y de organización necesarias para garantizar la seguridad de esos datos e información y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a la ley.

Esta obligación resulta aplicable tanto si la base de datos se encuentra en servidores localizados en la Superintendencia, como si se opta por su traslado a servidores en la Nube.

De esta forma, es importante que como parte del proyecto de "Sistemas en la Nube", se considere que el tratamiento de la información contenida en los sistemas que se trasladen, en particular el VES, esté sometida a mecanismos de seguridad física y lógica adecuados para garantizar la protección de la información almacenada.

Al respecto, se recomienda al Departamento de Tecnologías de Información definir claramente en el proyecto el tipo de Nube hacia el cual se hará el traslado,

considerando que, en principio, existen tres tipos: Nube pública, Nube privada y Nube híbrida, cada uno con diferentes niveles de protección.

Por otro lado, es importante que como parte del proyecto quede claramente establecido que aunque la información se mantenga en servidores en la Nube, esto no implica que la SUPEN, y en particular el Departamento de Tecnologías de la Información, pierda la condición de responsable de la base de datos, de manera que seguirá siendo el encargado de garantizar plenamente la seguridad e integridad de los centros de tratamiento, equipos, sistemas y programas. Esto implica definir claramente con la empresa proveedora del servicio los diferentes niveles de responsabilidad, la infraestructura a utilizar (nube pública, privada o híbrida) y, especialmente, las limitaciones necesarias en relación con el acceso y manipulación de la información.

VI. Conclusiones

A partir de los análisis de fondo realizado, esta Asesoría concluye que:

1. Como resultado del análisis realizado por esta Asesoría, no se encontró ninguna norma vigente que regule de manera específica la transferencia de sistemas a la Nube.
2. En materia de tratamiento de datos personales de los afiliados, así como otro tipo de información que de acuerdo con el artículo 67 de la LPT tenga carácter confidencial, la SUPEN, y en particular los responsables del manejo de las bases de datos, están obligados a tomar todas las medidas de índole técnica y de organización necesarias para garantizar la seguridad de esos datos e información y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a la ley.
3. Esta obligación resulta aplicable tanto si la base de datos se encuentra en servidores localizados en la Superintendencia, como si se opta por su traslado a servidores en la Nube.
4. Como parte del proyecto de "Sistemas en la Nube", debe considerarse que el tratamiento de la información contenida en los sistemas que se trasladen, en particular el VES, esté sometida a mecanismos de seguridad física y lógica adecuados para garantizar la protección de la información almacenada.
5. Aunque la información se mantenga en servidores en la Nube, esto no implica que la SUPEN, y en particular el Departamento de Tecnologías de la Información, pierda la condición de responsable de la base de datos, de manera que seguirá siendo el encargado de garantizar plenamente la seguridad e integridad de los centros de tratamiento, equipos, sistemas y programas.
6. Lo anterior implica definir claramente con la empresa proveedora del servicio los diferentes niveles de responsabilidad, la infraestructura a utilizar (nube pública, privada o híbrida) y, especialmente, las limitaciones necesarias en relación con el acceso y manipulación de la información.

Cordialmente,

Giselle Vargas Berrocal
Abogada encargada

Nelly Vargas Hernández
Directora
División de Asesoría Jurídica