30 de agosto de 2013
**PJD-15-2013**

Señor
Edgar Robles Cordero, *superintendente*
***Superintendencia de Pensiones***

Estimado señor:

Mediante tarea que consta en el Sistema de Trámites de esta Superintendencia de Pensiones (en adelante SUPEN) se solicitó a esta División: "*…analizar la normativa aplicable sobre la confidencialidad (manejo de información) en relación con la USA PATRIOT ACT (Ley Acta Patriota) específicamente con el Título II (Procedimientos Mejorados de Vigilancia)…"*.

En atención a esta solicitud, se emite el presente criterio jurídico.

## I. Antecedentes

Sobre el tema de los servidores en la "Nube" (conocido como cloud computing), la División Jurídica emitió el dictamen PJD-07-2011, del 13 de julio de 2011, mediante el cual se analizó*: "…la legalidad de tener la información de la Superintendencia de Pensiones (SUPEN) en Servidores en la Nube…".*

Dicho dictamen concluyó lo siguiente:

*"(...)*

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****…".* (el resaltado no pertenece al original).

Mediante oficio AI-CNS-019-2013, del 21 de junio de 2013, con el cual se adjunta el informe I-AI-CNS-18-2013, la Auditoría Interna del Consejo Nacional de Supervisión del Sistema Financiero señaló que el análisis realizado por la Asesoría Jurídica debió considerar la legislación de otros países que pudiera resultar aplicable. Adicionalmente, planteó una serie de recomendaciones para esta Superintendencia de Pensiones, así como la solicitud de indicar los responsables y plazos establecidos para ejecutar las acciones conducentes a su implementación.

En lo que aquí interesa en el citado informe se indicó: "*Este criterio no hace mención a las implicaciones sobre la confidencialidad de la información trasladada a la Nube, en razón de elementos tal como el domicilio del proveedor del servicio. Por ejemplo, el caso de la empresa Microsoft, que mantiene filiales e instalaciones en los Estados Unidos de Norte América, donde leyes como la USA PATRIOT ACT (Ley Acta Patriota), cuyo Título II (Procedimientos Mejorados de Vigilancia, del inglés Enhanced Surveillance Procedures) establecen la posibilidad de que dicho gobierno le requiera a cualquier empresa estadounidense, sea que esté instalada en su territorio o no, que suministre la información que le sea solicitada, sin importar la nacionalidad del propietario de esta. Una solicitud de esta naturaleza provocaría que la información de SUPEN que se encuentre almacenada en la Nube pueda ser expuesta a personas no autorizadas por nuestra legislación".* Y se emitió la recomendación*"…1.01 'Analizar la normativa aplicable sobre la confidencialidad de la información según sea la ubicación del proveedor y los servidores del servicio de la nube donde se almacena la información de SUPEN, con el fin de tomar las medidas correspondientes'…".*

Sobre el particular, la Superintendencia de Pensiones emitió el oficio SP-1000-2013, del 04 de julio de 2013, mediante el cual le indicó a la Auditoría Interna: *"….En relación con la* ***recomendación 1.01*** *(…) esta Superintendencia analizará la normativa aplicable sobre la confidencialidad (manejo de información) en relación con el USA Patriot Act (Ley Acta Patriota) específicamente con el Título II (Procedimientos Mejorados de Vigilancia). Para dicho análisis, este órgano supervisor va a requerir un plazo mínimo de 30 días hábiles; siendo el funcionario responsable la Directora de la División Jurídica, Nelly Vargas Hernández…".*

## II. Normativa aplicable

Sobre la confidencialidad de la información, la Ley de Protección al Trabajador (Ley N°7983) señala:

*"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 pertenece al original).

En línea con lo anterior, 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 (Ley N°7523), 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 N° 7337, de 5 de mayo de 1993".*

Teniendo en cuenta lo anterior, el 20 de febrero de 2012 la Superintendencia de Pensiones suscribió varios documentos contractuales[1] con la empresa Microsoft, dirigidos a la contratación de servicios online. El documento *"Microsoft Business and Services Agreement"*, en su apartado 3 se refiere al tema de la confidencialidad de la información en los siguiente términos:

*"**3. Confidencialidad.** Resumen: Cada una de las partes acepta no utilizar la información Confidencial de la otra parte, salvo que sea necesario para propósitos del contrato entre las partes. Cada una de las partes acepta realizar los pasos razonables para proteger esa información y cooperar entre sí en caso de que sea revelada.*

- ***a. Lo que incluye**. 'Información Confidencial' es información no pública, know-how y de Secretos Empresariales en cualquier forma que:*
  ***(i)** se designen como 'confidenciales';*
  ***(ii)** una persona razonable conoce o razonablemente debería comprender que es confidencial; o*
  ***(iii)** incluye información no pública relativa a los productos o clientes de cualquiera de las partes, marketing y promociones o los términos negociados de los contratos de Microsoft.*

[1] En el año 2012, la Superintendencia de Pensiones suscribió con Microsoft los siguientes documentos contractuales: Microsoft Business and Services Agreement (X20-02001), Contrato Enterprise (X20-02023), Inscripción a Enterprise Subscription (directa) (X20-02214), Corrección de Enterprise Subscriction (M92-6-5F5DLHZS2), Corrección de Enterprise Suscription (CTM-6-5F5DLHZS2), Hoja de precios del cliente del contrato de Enterprises Subcription (0003477.003) y el Formulario de Selección de Productos (X20-02720).

***b. Lo que no incluye**. Aunque los siguientes tipos de información están marcados, no son Información Confidencial. Información que:*
***(i)** es o se vuelve disponible para el público sin un incumplimiento de este contrato;*
***(ii)** era conocida legalmente por el receptor de la información sin estar sujeto a ninguna obligación de mantener su confidencialidad;*
***(iii)** sea recibida de otra fuente que pueda revelarla legalmente y que no esté sujeta a ninguna obligación de mantener su confidencialidad;*
***(iv)** sea desarrollada de manera independiente; o*
***(v)** sea un comentario o una sugerencia que una de las partes ofrece voluntariamente sobre el negocio, los productos o los servicios de la otra.*

***c. Tratamiento de la Información Confidencial.***
***(i) En general.** Con sujeción a los demás términos de este contrato, cada una de las partes acuerda que:*
- *no revelará la Información Confidencial de la otra a terceros y*
- *usará y revelará la Información Confidencial de la otra sólo para fines derivados de la relación comercial mutua entra las partes.*

***(ii) Precauciones de seguridad.** Con sujeción a los demás términos de este contrato cada una de las partes acuerda que:*
- *realizará los pasos razonables para proteger la Información Confidencial de la otra parte, debiendo ofrecer estos pasos como mínimo la misma protección que los que la parte realice para proteger su propia Información Confidencial.*
- *notificará a la otra de inmediato, una vez descubierto, cualquier uso o revelación de Información Confidencial y*
- *cooperará con la otra parte para ayudarla a recuperar el control de la Información Confidencial y prevenir otro uso y revelación no autorizada de ella.*

***(iii) Intercambio de Información Confidencial con Filiales y representantes.***
- *Un 'representante' es un empleado, contratista, asesor o consultor de una de las partes o de una de las Filiales de las partes.*
- *Cada una de las partes podrá revelar esa Información Confidencial de la otra a sus Representantes (que podrán, a su vez, revelar esa Información Confidencial a otro de los Representantes de esa parte) sólo si dichos Representantes necesitan conocerla para fines derivados de la relación comercial entre las partes. Antes de hacerlo, cada una de las parte debe:*
  1) *asegurarse de que las Filiales y Representantes estén obligados a proteger la Información Confidencial en términos coherentes con este contrato y*
  2) *aceptar la responsabilidad por el uso de la Información Confidencial de cada Representante.*
- *Ninguna de las partes está obligada a restringir las tareas de los Representantes que tienen acceso a Información Confidencial. Ninguna de las partes podrá controlar la información entrante que la otra le revele durante su trabajo en conjunto o lo que los Representantes de esa parte pueden recordar, incluso son apuntes u otras ayudas. Cada una de las partes acuerda que el uso de la información en las memorias de los Representantes en el desarrollo o implementación de los respectivos productos o servicios de las partes no crea responsabilidad alguna bajo este contrato o derecho de*
- *secretos empresariales, y cada una de las partes acuerda limitar lo que revela a la otra adecuadamente.*

***(iv) Revelación de Información Confidencial si lo exige la ley.*** *Cada una de las partes podrá revelar la Información Confidencial de la otra si se le exige que cumpla una orden judicial o cualquier petición gubernamental que tenga fuerza de ley. Antes de hacerlo, cada una de las partes debe buscar el nivel más alto de protección disponible y, cuando sea posible, notificar con suficiente anterioridad a la otra para que tenga una oportunidad razonable de buscar una orden de protección judicial.*

***d. Duración de las obligaciones respecto de la Información Confidencial.*** *Salvo en la forma permitida en los términos antes descritos, ninguna de las partes usará o revelará la Información Confidencial de la otra durante 5 años después de recibirla. El período de 5 años no se aplica si la legislación aplicable exige un período más largo o si los Derechos de Uso de los productos establecen un requisito más específico…".*

## III. Análisis de la consulta

Se solicitó a la División Jurídica referirse a lo siguiente: *"Analizar la normativa aplicable sobre la confidencialidad de la información según sea la ubicación del proveedor y los servidores del servicio de la nube donde se almacena la información de SUPEN, con el fin de tomar las medidas correspondientes*". De acuerdo con lo anterior, este órgano supervisor acordó analizar la normativa aplicable sobre la confidencialidad (manejo de información) en relación con el USA Patriot Act (Ley Patriota) específicamente con el Título II (Procedimientos Mejorados de Vigilancia) al cual se hace referencia en el informe de la Auditoría Interna supra citado.

### 1. Sobre la confidencialidad

Una información confidencial es básicamente la que se pone en conocimiento de alguien, con intención de que ésta no sea revelada a nadie. Al respecto señala la doctrina: *"…Normalmente, una información confidencial es aquélla que se revela a alguien con la intención de que no sea revelada a los demás sin consentimiento del interesado (…) La confidencialidad representa una manifestación de la 'confianza' que se ha depositado en un tercero, que será quien oculte con la complicidad de la persona lo que le ha sido revelado, consiste en una exteriorización de los comportamientos y actitudes como expresión de las propias relaciones humanas, si bien con la garantía y compromiso de que lo que se ha compartido no será facilitado al conocimiento general…"*[2]. La confidencialidad lleva implícita, por lo tanto, la obligación de guardar una información o documentación suministrada.

No obstante lo anterior, es necesario indicar que la confidencialidad, como principio, **puede verse vulnerada en aquellos casos en que el ordenamiento ordene u autorice la posibilidad de revelar la información suministrada**.

En el dictamen C-007-2005, del 12 de enero de 2005 la Procuraduría General de la República se refirió a este tema indicando que: *"…La confidencialidad conlleva una obligación para toda persona distinta de su titular de guardar la reserva necesaria sobre una información o documentación que le ha sido proporcionada. Por consiguiente, quien ha recibido la información está impedido de divulgarla o de*

[2] A. HERRAN ORTIZ
La violación de la intimidad en la protección de los datos personales, Dykinson S. L., 1999, página 13.

*darla a conocer por algún otro medio a otras personas,* ***salvo que el ordenamiento lo autorice****.* ***Esa excepción implicaría, entonces, la existencia de un interés público superior que justifique dejar sin efecto la confidencialidad****.* ***Si ese interés público no existe, la información recabada sólo puede ser empleada para los fines por los cuales se entregó u obtuvo, sin posibilidad de emplearse para otros objetivos****…"* (El resaltado no pertenece al original).

En el mismo sentido, en el dictamen C-019-2010, del 25 de enero de 2010, el órgano asesor señaló: *"…En nuestro ordenamiento la información confidencial se constituye en un límite para el acceso a la información que consta en oficinas públicas. Por ende, al derecho de acceso a la información pública.* ***Es por ello que la confidencialidad debe ser definida por el constituyente o el legislador****…"* (El resaltado no pertenece al original).

En este contexto, y en lo que se refiere a la Superintendencia de Pensiones y los entes sujetos a su fiscalización, de especial interés resulta lo indicado en el artículo 67 de la Ley de Protección al Trabajador, y en el artículo 32 de la Ley Orgánica del Banco Central de Costa Rica.

En el primer caso, dicho artículo se refiere a la confidencialidad que debe guardarse respecto de la información de las inversiones de un ente regulado por la SUPEN, que aún no haya sido divulgada oficialmente en el mercado; así como de la información registrada en las cuentas individuales de los afiliados, la cual no puede ser suministrada a terceros excepto en los casos previstos en la ley.

En el segundo caso, dicho artículo plantea algunas excepciones legales al principio de confidencialidad, que resulta importante tener en cuenta para efectos de analizar la inquietud planteada por la Auditoría Interna del CONASSIF, a saber:

*"Artículo 132.- Prohibición*
*Queda prohibido al Superintendente, al Intendente, a los miembros del Consejo Directivo, a los empleados, asesores y a cualquier otra persona, física o jurídica, que preste servicios a la Superintendencia en la regularización o fiscalización de las entidades financieras,* ***dar a conocer información relacionada con los documentos, informes u operaciones de las entidades fiscalizadas****. La violación de esta prohibición será sancionada según lo dispuesto en el artículo 203 del Código Penal. Tratándose de funcionarios de la Superintendencia constituirá, además, falta grave para efectos laborales.* ***Se exceptúan de la prohibición anterior****:*
*a) La información que la Superintendencia deba brindar al público en los casos y conforme a los procedimientos expresamente previstos en esta ley.*
*b)* ***La información requerida por orden de autoridad judicial competente.***
*c) La información solicitada por la Junta Directiva del Banco Central, por acuerdo de por lo menos cinco de sus miembros, en virtud de ser necesaria para el ejercicio de las funciones legales propias de ese órgano. En estos casos, los miembros de la Junta Directiva y demás funcionarios del Banco Central estarán sujetos a la prohibición indicada en el párrafo primero de este artículo.*
*d) La información de interés público, calificada como tal por acuerdo unánime del Consejo Directivo.*
*e) La información que requiera la Contraloría General de la República en ejercicio de sus atribuciones.*
*f)* ***La información que requiera la (UIF), del Instituto Costarricense sobre Drogas, en ejercicio de sus atribuciones para combatir la legitimación de capitales y el financiamiento al terrorismo****.*

*Salvo en los casos que esta ley establece, ningún funcionario de la Superintendencia o miembro del Consejo Directivo podrá hacer público su criterio acerca de la situación financiera de las entidades fiscalizadas. Sin perjuicio de las sanciones aplicables, el Superintendente deberá informar al público, por los medios y en la forma que estime pertinentes, sobre cualquier persona, física o jurídica, nacional o extranjera, que realice actividades de intermediación financiera en el país sin estar autorizada de conformidad con esta ley…"* (El resaltado no pertenece al original).

Se desprende del inciso b) de esta norma, que una excepción a la confidencialidad se presenta cuando la información es requerida por orden de autoridad judicial competente. Media en este caso un interés superior, que justifica que las prohibiciones contenidas en la Ley en esta materia cedan frente al juez, el cual puede solicitar la información que requiera en el ejercicio de sus potestades y competencias.

En este sentido, en el dictamen C-003-2003 del 14 de enero de 2003, la Procuraduría General de la República indicó sobre este particular que: *"…La confidencialidad se ejerce en relación con información y documentos privados y significa una obligación para toda persona distinta de su titular de guardar la reserva necesaria sobre dicha información o documentación. Lo cual implica que si el derecho habiente confía dicha información o documentos a un tercero, normalmente la Administración, ésta está impedida de divulgarla o a darla a conocer por algún otro medio a otras personas,* ***salvo que el ordenamiento lo autorice***. ***Esa excepción implicaría, entonces, que hay un interés público superior que justifica dejar sin efecto la confidencialidad****…".* (El resaltado no pertenece al original).

Por su parte, la Sala Constitucional ha señalado: *"En efecto,* ***de este texto se desprende, en forma, si no expresa, al menos inequívoca la exclusividad****- y, más aún, la universalidad- de* ***la función jurisdiccional en el Poder Judicial****,* ***con la consiguiente interdicción de cualquier otro con ese carácter y cualquiera que sea su denominación****; con lo cual nuestra Constitución hizo indivisible lo jurisdiccional y lo judicial …"* (el resaltado no pertenece al original) sentencia N° 1148-90, de las diecisiete horas del veintiuno de setiembre de mil novecientos noventa; *"…El principio constitucional de exclusividad o reserva de jurisdicción en el ejercicio de la función jurisdiccional, se encuentra establecido en el artículo 153 de la Constitución Política que estatuye "(...)* ***Corresponde al Poder Judicial, además de las funciones que esta Constitución le señala, conocer de las causas*** *(…) resolver definitivamente sobre ellas y ejecutar las resoluciones que pronuncie".* ***Este precepto constitucional también enuncia el núcleo duro de la función materialmente jurisdiccional, la cual le corresponde ejercer, privativa y exclusivamente, a ese Poder de la República a través de las diversas Salas de la Corte Suprema de Justicia, los tribunales y juzgados que establezca la ley*** *(artículo 152 ibidem). De este modo,* ***el principio de reserva de jurisdicción significa que los tribunales han sido instituidos, exclusivamente, para ejercer esa función material, a través del dictado de sentencias con fuerza de verdad legal para dirimir una controversia o litigio entre las partes*** *–extremo que no excluye la terminación anormal o anticipada de los procesos a través de otro tipo de resoluciones- y de su debida ejecución…"* (El resaltado no pertenece al original, sentencia N°7965-06, de las dieciséis horas con cincuenta y ocho minutos del treinta y uno de mayo de 2006).

La obligación de entregar la información cuando es requerida por autoridad judicial competente, aplica para SUPEN no importa si la información está almacenada en servidores propios, o en la Nube. No obstante, es importante reiterar que en el caso de almacenamiento en la Nube, el

contrato suscrito por la SUPEN y por Microsoft señala que: "…*Cada una de las partes podrá revelar la Información Confidencial de la otra* ***si se le exige que cumpla una orden judicial*** *o* ***cualquier petición gubernamental que tenga fuerza de ley****. Antes de hacerlo, cada una de las partes debe buscar el nivel más alto de protección disponible y, cuando sea posible, notificar con suficiente anterioridad a la otra para que tenga una oportunidad razonable de buscar una orden de protección judicial..."* (El resaltado no pertenece al original). Nótese que la solicitud siempre se sujeta a la Ley, e implica que sea formulada por funcionarios judiciales investidos para tal efecto.

## 2. Sobre la información que se encuentra en la "Nube"

En los cuadros adjuntos se detallan las aplicaciones que mantiene SUPEN, así como su situación con respecto al almacenamiento en la Nube:

**Ventanilla Electrónica de Servicios (VES)**

| # | Nombre del sistema | Descripción | En la Nube | Base de Datos | Observaciones |
|---|---|---|---|---|---|
| La | Transferencia y Carga de Información | Permite la transferencia de archivos de saldos contables, movimientos de afiliados, de las Operadoras y Fondos Colectivos. | Si | SQL Server y ORACLE | La Base de Datos ORACLE esta en nuestros servidores. |
| 2 | Sistema de Incentivos Fiscales | Permite a las entidades supervisadas calcular el monto del incentivo fiscal que se debe deducir a los afiliados que se retiran de los fondos complementarios. | Si | SQL Server | |
| 3 | Sistema de Actas Electrónicas | Lleva el control de las actas generadas en comités de riesgos, inversiones de entidades supervisadas. | Si | SQL Server y ORACLE | La Base de Datos ORACLE esta en nuestros servidores. |
| 4 | Sistema de Valoración de Riesgo (VaR) | Permite calcular el riesgo que existe en las carteras de inversiones de las entidades supervisadas. | Si | SQL Server y ORACLE | La Base de Datos ORACLE esta en nuestros servidores. |
| 5 | Sistema de Administración de Seguridad (SAS) | Permite a las entidades supervisadas administrar la seguridad de sus funcionarios, para interactuar con el portal Ves y a su vez también permite a la SUPEN designar los encargados de las entidades para administrar dicha seguridad. | Si | SQL Server | |
| 6 | Sistema de Información Cualitativa (SIC) | Permite registrar los datos relevantes de las entidades supervisadas, como su estructura organizacional, comités, etc. | Si | SQL Server y ORACLE | La Base de Datos ORACLE esta en nuestros servidores. |
| 7 | Sistema Electrónico de Compensación (SEC) | Permite la compensación de montos transferidos de una entidad a otra, mediante la libre transferencia de afiliados. | Si | SQL Server | |
| 8 | Servicio de Documentación | Se usa para subir archivos tales como manuales, etc. | Si | SQL Server | |
| 9 | Servicio de Consulta | Se implementaron varias consultas que se realizan al sistema de afiliados e inversiones. | Si | SQL Server y ORACLE | La Base de Datos ORACLE esta en nuestros servidores. |
| 10 | Servicios de Apoyo a Inversiones | Se utiliza para registrar las ventas parciales utiliza el sistema de inversiones. | Si | SQL Server y ORACLE | La Base de Datos ORACLE esta en nuestros servidores. |

**Sistemas institucionales en Oracle**

| # | Nombre del sistema | Descripción | En la Nube | Base de Datos | Observaciones |
|---|---|---|---|---|---|
| 11 | Sistema de Afiliados y Pensionados | Provee las facilidades necesarias para el mantenimiento y consulta de datos relacionados con: afiliados, pensionados, aportes, cotizaciones, etc., de los diferentes regímenes de pensión complementaria y los regímenes de capitalización individual. | No | ORACLE | La Base de Datos ORACLE esta en nuestros servidores. |
| 12 | Sistema de Saldos Contables e Inversiones | Provee las facilidades necesarias para el mantenimiento y consulta de datos relacionados con: los saldos contables e inversiones de los diferentes regímenes de pensión complementaria y los regímenes de capitalización individual. | No | ORACLE | La Base de Datos ORACLE esta en nuestros servidores. |

**Sistemas institucionales en Visual Basic .NET**

| # | Nombre del sistema | Descripción | En la Nube | Base de Datos | Observaciones |
|---|---|---|---|---|---|
| 13 | **Sistema de Calidad** | Se utiliza para llevar el control documental de todos los procedimientos, instrucciones de trabajo y formularios del Sistema de Gestión Documental de la SUPEN. | SI | SQL Server | |
| 14 | **Sistema de Trámites** | Implementa el flujo básico que corresponde a la gestión de trámites, considerando la creación de encargos, documentos y tareas, así como el registro de anotaciones en cada nivel definido y la posibilidad de adjuntar documentos. | SI | SQL Server | |
| 15 | **Sistema de Help Desk** | Permite a los funcionarios de la SUPEN, registrar solicitudes de soporte técnico, para ser atendidas por el Departamento de TI. | SI | SQL Server | |
| 16 | **Sistema de Inventarios** | Permite llevar el control de los equipos y mobiliario asignado a los funcionarios de la SUPEN. | Si | SQL Server | |
| 17 | **Sistema de Suministros** | Permite la solicitud, mantenimiento y consulta de los diferentes artículos, equipos o utensilios que pueden ser solicitados por los funcionarios al área de comunicación y servicios, como por ejemplo: lapiceros, cuadernos, CDs, DVDs, etc. | No | SQL Server | Se inició el pase a la Nube |
| 18 | **Sistema de Presupuesto** | Se utiliza para llevar el presupuesto de la SUPEN | SI | SQL Server | |
| 19 | **Inteligencia de Negocios para Afiliados (DataWarehouse)** | Se utiliza para la generación de reportes ejecutivos, referentes a los datos de afiliados de los entes supervisados. | No | SQL Server y ORACLE | La Base de Datos ORACLE esta en nuestros servidores. |

**Página Web de la SUPEN**

| # | Nombre del sistema | Descripción | En la Nube | Base de Datos | Observaciones |
|---|---|---|---|---|---|
| 20 | **Página Web** | Página desarrollada por Hermes Soft que consta de varias páginas. | SI | SQL Server | |

**Portal Institucional**

| # | Nombre del sistema | Descripción | En la Nube | Base de Datos | Observaciones |
|---|---|---|---|---|---|
| 21 | **Portal Institucional** | Desarrollado en Sharepoint, que se utiliza como Intranet de la SUPEN. | Si | SQL Server | El Sharepoint utiliza una base de datos SQL Server que esta en la nube |

Se desprende de lo anterior que en la actualidad la información que SUPEN almacena en la Nube es la siguiente:

**a.** Ventanilla electrónica de Servicios (VES).
**b.** Los sistemas institucionales en Visual Basic.NET: sistemas de calidad, sistemas de trámites, sistema de help desk, sistema de inventarios y sistema de presupuesto.
**c.** Página web de la SUPEN y
**d.** Portal Institucional.

A la fecha no se encuentra en la Nube la información contenida en los sistemas institucionales en Oracle, el cual incluye el sistema de afiliados y pensionados, y el sistema de saldos contables e inversiones, no obstante, se están realizando los ajustes necesarios para hacer su pase a la Nube en los próximos meses.

### 3. Sobre la Ley Patriota de los Estados Unidos de América

La Ley Patriota de los Estados Unidos de América (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism), fue emitida en octubre de 2001, en razón de los ataques terroristas que tuvieron lugar el 11 de setiembre de ese año. Su objetivo es contrarrestar el lavado de dinero, el espionaje, el terrorismo y su financiamiento.

A pesar de que el informe de la Auditoría Interna no indica expresamente cuáles son las normas de la Ley Patriota que motivan su inquietud, se revisó la totalidad de esa Ley, con el fin de determinar las posibles implicaciones sobre la confidencialidad de la información trasladada a la Nube, en razón de la sujeción de Microsoft a esa normativa. En ese sentido, de interés para este caso resultan las modificaciones hechas por la Ley Patriota a las Reglas Federales de Procedimientos, y a la Ley de Vigilancia de Inteligencia Extranjera.

En el primer caso se dispone lo siguiente:

*"Sección. 203. Autoridad para compartir Información Criminal Investigativa*
*(d) Información de Inteligencia Extranjera*
*(1) En general, y sin perjuicio de cualquier otra previsión legal, será legítimo que cualquier información obtenida sobre inteligencia extranjera o contrainteligencia (términos definidos en la sección 3 de la Ley de Seguridad Nacional de 1947) sea revelada a cualquier oficial de implementación de la ley Federal, migración, defensa nacional o de seguridad nacional para los efectos de asistir al oficial que recibe la información en la ejecución de sus deberes oficiales. Cualquier oficial Federal que reciba información relacionada con esta disposición puede usar dicha información solo si es necesario para la ejecución de sus deberes oficiales sujeto a las disposiciones sobre la revelación no autorizada de dicha información.*
*(2) Definiciones: En esta subsección el término "Información de Inteligencia extranjera" significa:*
*(A) Información, relativa o no a una persona estadounidense relacionada con la habilidad de los Estados Unidos de protegerse contra:*
*(i) Ataques potenciales o actuales u otros actos graves de hostilidad de un poder extranjero o un agente de un poder extranjero.*
*(ii) Sabotaje o terrorismo internacional por un poder extranjero o un agente de un poder extranjero.*
*(iii) Actividades de inteligencia clandestinas por una red o servicio de inteligencia de un poder extranjero o por un agente de un poder extranjero, o*
*(B) Información, relativa o no a una persona estadounidense en relación con un poder extranjero o territorio extranjero sobre:*
*(i) La defensa nacional o la seguridad de los Estados Unidos, o*
*(ii) El desarrollo de las relaciones exteriores de los Estados Unidos".*

En el segundo caso, se regula el acceso a archivos y otros ítems sujetos a la Ley de Vigilancia de Inteligencia Extranjera como sigue:

*"Sección. 215. Acceso a archivos y otros items bajo la Ley de Vigilancia de Inteligencia Extranjera*
*El Título V de la Ley de Vigilancia de Inteligencia Extranjera de 1978 es enmendada eliminando las secciones 501 al 503 e insertando lo siguiente:*
*"SEC. 501. Acceso a ciertos archivos de negocios para investigaciones de Inteligencia Extranjera y Terrorismo Internacional.*
*(a) (1) El Director del FBI o su designado (cuyo rango no puede ser inferior que el de Asistente Agente Especial a Cargo) puede hacer una solicitud de una orden requiriendo la entrega de cosas tangibles (incluyendo libros, registros, papeles, documentos y otros ítems) para una investigación que proteja contra terrorismo internacional o actividades clandestinas de inteligencia provisto que dicha investigación sea dirigida contra un estadounidense no sea conducida únicamente sobre la base de actividades protegidas por la primera enmienda de la Constitución.*

*(2) Una investigación conducida bajo las disposiciones de esta sección debe:*
*(a) Ser conducida bajo los lineamientos aprobados por el Fiscal General bajo orden ejecutiva 12333 (o una posterior), y*
*(b) No ser dirigida contra un estadounidense únicamente sobre la base de actividades protegidas por la primera enmienda de la Constitución.*
*(b) Toda solicitud hecha bajo esta sección,*
*(1) Deberá ser dirigida a:*
*(a) Un Juez de la corte establecida por la sección 103 (a) (Una corte para escuchar solicitudes y emitir órdenes); o*
*(b) Un Juez Magistrado de los Estados Unidos (capítulo 43 del título 28 del Código de los Estados Unidos), el cual es públicamente designado por el Magistrado Principal de los Estados Unidos y que tiene el poder para escuchar solicitudes y emitir órdenes para la entrega de cosas tangibles bajo esta sección en nombre de un juez de la corte establecida por la sección 103 (a) (Una corte para escuchar solicitudes y emitir órdenes).*
*(2) Deberá contener:*
*Debe especificar que los archivos en cuestión son pretendidos por una investigación autorizada de acuerdo a la subsección (a) (2) para obtener información de inteligencia extranjera no relacionada con una persona estadounidense o para proteger en contra de terrorismo internacional o actividades de inteligencia clandestinas.*
*(c) (1) Tras una solicitud presentada en virtud del presente apartado, el juez emitirá una orden ex parte conforme a lo solicitado, o modificado, aprobando la liberación de los archivos si el juez considera que la solicitud cumple con los requisitos de esta sección.*
*(2) Una orden bajo este inciso no divulgará que es expedida para los fines de una investigación descrita en la subsección (a).*
*(d) Ninguna persona deberá revelar a cualquier otra persona (excepto las personas necesarias para producir las cosas tangibles en esta sección) que el FBI ha solicitado u obtenido información tangible bajo esta sección.*
*(e) Una persona que, de buena fe, entrega cosas tangibles en virtud de una orden en virtud de la presente sección no será responsable ante cualquier otra persona por dicha entrega. Dicha entrega no se considerará que constituya una renuncia a cualquier fuero o privilegio de otro procedimiento o contexto".*

De las normas transcritas es posible concluir lo siguiente:

1. De acuerdo con la reforma introducida por la Ley Patriota a las Reglas Federales de Procedimientos, la información revelada a cualquier oficial de implementación de la ley federal de migración, defensa nacional o de seguridad nacional, puede ser usada solo si es necesaria para la ejecución de sus deberes oficiales, sujeto a las disposiciones sobre la revelación no autorizada de dicha información.

2. Se entiende por información de inteligencia extranjera:

   a) información relativa o no a una persona estadounidense relacionada con la habilidad de los Estados Unidos de protegerse contra: ataques potenciales o actuales u otros actos graves de hostilidad de un poder extranjero o un agente de un poder extranjero; sabotaje o terrorismo internacional por un poder extranjero o un agente de un poder

extranjero; actividades de inteligencia clandestinas por una red o servicio de inteligencia de un poder extranjero o por un agente de un poder extranjero, o

b) Información, relativa o no, a una persona estadounidense en relación con un poder extranjero o territorio extranjero sobre: la defensa nacional o la seguridad de los Estados Unidos, o el desarrollo de las relaciones exteriores de los Estados Unidos.

3. Según la reforma a la Ley de Vigilancia de Inteligencia Extranjera, para el acceso a ciertos archivos de negocios para investigaciones de inteligencia extranjera y terrorismo internacional, el Director del FBI o su designado puede hacer una solicitud de una orden requiriendo la entrega de cosas tangibles (incluyendo libros, registros, papeles, documentos y otros ítems) para una investigación que proteja contra terrorismo internacional o actividades clandestinas de inteligencia.

   En este caso la solicitud debe cumplir ciertos *requisitos*:

   a) Debe ser tener relación con una investigación conducida bajo los lineamientos aprobados por el Fiscal General bajo orden ejecutiva 12333
   b) Debe ser dirigida a un juez de la corte establecida por la sección 103 (a) (una corte para escuchar solicitudes y emitir órdenes); o un Juez Magistrado de los Estados Unidos
   c) Debe especificar que los archivos en cuestión son pretendidos por una investigación autorizada de acuerdo a la subsección (a) (2) para obtener información de inteligencia extranjera no relacionada con una persona estadounidense o para proteger en contra de terrorismo internacional o actividades de inteligencia clandestinas.
   d) Corresponde al juez emitir una orden ex parte conforme a lo solicitado, o modificado, aprobando la liberación de los archivos si el juez considera que la solicitud cumple con los requisitos.
   e) Ninguna persona deberá revelar a cualquier otra persona (excepto las personas necesarias para producir las cosas tangibles en esta sección) que el FBI ha solicitado u obtenido información tangible bajo esta sección.
   f) Una persona que, de buena fe, entrega cosas tangibles en virtud de una orden como la indicada no será responsable ante cualquier otra persona por dicha entrega. Dicha entrega no se considerará que constituya una renuncia a cualquier fuero o privilegio de otro procedimiento o contexto.

En relación con lo indicado por la Auditoría Interna en el informe I-AI-CNS-18-2013, considera esta Asesoría que las normas transcritas sí pueden implicar un riesgo para la información que SUPEN almacena en la Nube, en especial una vez que se utilice esta herramienta para almacenar la información contenida en el sistema de afiliados y pensionados, y el sistema de saldos contables e inversiones, pues es lo cierto que Microsoft se encuentra sujeta a la Ley Patriota, y por tanto a las disposiciones sobre acceso a archivos y otros ítems previstas en la Ley de Vigilancia de Inteligencia Extranjera.

No obstante lo anterior, interesa determinar si este riesgo implicaría la imposibilidad de recurrir a la Nube como un medio para el almacenamiento de la información indicada, o si, por el contrario, este riesgo puede ser mitigado tomando las medidas correspondientes.

**4. Sobre los riesgos que conlleva almacenar la información en la Nube y su mitigación**

El riesgo es, básicamente, la probabilidad de un potencial peligro o perjuicio que pueda dañar a algo o alguien. Por su naturaleza, los riesgos pueden disminuirse, pero no pueden ser eliminados en su totalidad.

Partiendo de este principio, en este apartado se analiza el posible riesgo que supone el hecho de que SUPEN almacene información en la Nube.

Al respecto, y tal y como se ha mencionado en líneas anteriores, la confidencialidad es un principio que cede ante la Ley, o ante la solicitud de una autoridad judicial; partiendo de esa premisa, siempre existe el riesgo de que la información resguardada bajo este principio sea eventualmente conocida. Sin embargo, debe tomarse en consideración que cuando la información es solicitada para dichos fines (judiciales o por Ley expresa) la información se utiliza únicamente para lo que señale la Ley y el mandato judicial, es decir, no puede ser utilizada para fines personales ni de terceros.

Esto aplica tanto para la información almacenada en los servidores de la SUPEN, como para la información almacenada en la Nube.

Ahora bien, se entiende que el motivo de preocupación de la Auditoría Interna se encuentra referido a que en virtud de lo dispuesto en la Ley Patriota esta información pueda "*ser expuesta a personas no autorizadas por nuestra legislación".*

Al respecto, es importante tener presente que la Ley Patriota no se aparta de lo indicado por la legislación y jurisprudencia administrativa costarricense a que se hizo referencia en el punto uno de este análisis, pues sujeta la solicitud de información a la participación de una autoridad judicial, y siempre en el marco de una investigación realizada en relación con temas de terrorismo internacional o actividades de inteligencia clandestinas. No obstante lo anterior, es claro que se trata de una autoridad judicial extranjera.

Ahora bien, ¿es posible por medios tecnológicos, o de otra índole, disminuir o mitigar el riesgo que conlleva lo dispuesto en la Ley Patriota en relación con la entrega de la información confidencial que se encuentra en la Nube? En este contexto es importante traer a colación las medidas adoptadas por la SUPEN y por Microsoft para disminuir este riesgo.

Sobre el particular, y reconociendo la responsabilidad compartida a que se ha hecho referencia, la Superintendencia de Pensiones ha procurado mitigar los posibles riesgos que conlleva el almacenamiento de información en la nube de la siguiente forma:

i. Ha suscrito diferentes acuerdos de servicio con la empresa Microsoft, ello con la finalidad de definir claramente los responsables de atender las eventualidades que se presenten.
ii. Adquirió el certificado SSL con el protocolo HTTPS, lo anterior con la finalidad que los datos que se encuentran en la "Nube" se transmitan encriptados y con ello se pueda dar garantía que el sitio es seguro.
iii. Requiere la autenticación del usuario, para ello uno de los métodos implementados es el uso de certificado digital (firma digital).

En abono de lo anterior, los centros de datos de la empresa Microsoft, los cuales se encuentran geográficamente dispersos, cumplen con los estándares del sector en materia de seguridad y confiabilidad, con la norma ISO/IEC 27001:2005.

Nótese que las anteriores medidas de disminución de riesgo son preventivas, y se han adoptado con el fin de mantener la información que se encuentra en la Nube lo más segura posible.

Por otro lado, no debe perderse de vista que desde el punto de vista contractual, SUPEN y Microsoft cuentan con reglas claras a aplicar en caso de que a la segunda le sea requerida información en virtud de lo dispuesto en la Ley Patriota.

Claramente en dicho instrumento se indica que: *"Cada una de las partes podrá revelar la Información Confidencial de la otra si se le exige que cumpla una orden judicial o cualquier petición gubernamental que tenga fuerza de ley.* ***Antes de hacerlo, cada una de las partes debe buscar el nivel más alto de protección disponible y, cuando sea posible, notificar con suficiente anterioridad a la otra para que tenga una oportunidad razonable de buscar una orden de protección judicial****..."* (El resaltado no pertenece al original). Nótese que la solicitud siempre se sujeta a la Ley, e implica que sea formulada por funcionarios judiciales investidos para tal efecto. Además, la notificación prevista en esta cláusula tiene como fin posibilitar a la otra parte, en este caso la SUPEN, para que tenga una oportunidad razonable de buscar una orden de protección judicial.

Especial mención merece en este sentido el tema de la encriptación, y sobre todo a propósito de lo señalado en el numeral d) de la sección 501 de la Ley de Vigilancia de Inteligencia Extranjera, según fue reformada por la Ley Patriota, en el cual se indica: *Ninguna persona deberá revelar a cualquier otra persona (****excepto las personas necesarias para producir las cosas tangibles en esta sección****) que el FBI ha solicitado u obtenido información tangible bajo esta sección*. Es de prever que en caso de requerirse el acceso a información almacenada por la SUPEN en la Nube, deba recurrirse a este órgano, no sólo para conocer la naturaleza de dicha información, pues Microsoft

no cuenta con ese grado de detalle, sino también para que, si es del caso, se colabore proporcionando la clave necesaria para que ésta pueda ser analizada.

El contrato de cita establece, además, que cada una de las partes acepta realizar los pasos razonables para proteger esa información y cooperar entre sí en caso de que sea revelada. De acuerdo con lo anterior se indica:

*" (...)*

***e. Tratamiento de la Información Confidencial.***

***(i) En general.*** *Con sujeción a los demás términos de este contrato, cada una de las partes acuerda que:*

- *no revelará la Información Confidencial de la otra a terceros y*
- *usará y revelará la Información Confidencial de la otra sólo para fines derivados de la relación comercial mutua entra las partes.*

***(ii) Precauciones de seguridad.*** *Con sujeción a los demás términos de este contrato cada una de las partes acuerda que:*

- *realizará los pasos razonables para proteger la Información Confidencial de la otra parte, debiendo ofrecer estos pasos como mínimo la misma protección que los que la parte realice para proteger su propia Información Confidencial.*
- *notificará a la otra de inmediato, una vez descubierto, cualquier uso o revelación de Información Confidencial y*
- *cooperará con la otra parte para ayudarla a recuperar el control de la Información Confidencial y prevenir otro uso y revelación no autorizada de ella.*

***f. Duración de las obligaciones respecto de la Información Confidencial.*** *Salvo en la forma permitida en los términos antes descritos, ninguna de las partes usará o revelará la Información Confidencial de la otra durante 5 años después de recibirla. El período de 5 años no se aplica* ***si la legislación aplicable exige un período más largo*** *o si los Derechos de Uso de los productos establecen un requisito más específico…".*

En este contexto, no debe perderse de vista el compromiso público asumido por Microsoft en el sitio http://www.windowsazure.com/es-es/support/trust-center/faq/, cuyo texto es el siguiente: *"… **¿Qué sucede si terceros le solicitan mis datos de cliente a Microsoft con fines legales u otros propósitos? ¿Qué hará Microsoft si recibe una citación en la que se solicitan datos de clientes?** Microsoft cree que sus clientes deben controlar su propia información, esté almacenada de forma local o en un servicio en la nube. En consecuencia, **no revelaremos los datos de los clientes a terceros** (ni siquiera a una autoridad judicial, otra entidad gubernamental o litigante civil) **salvo que usted lo indique o por imperativo legal**. Si terceras partes se pusiesen en contacto con nosotros solicitando datos de clientes, **les indicaríamos que se los solicitasen directamente a ellos**. A tal fin, les podríamos proporcionar información de contacto básica. **Si nos viésemos obligados a revelar sus datos de cliente a terceros, emplearíamos todos los esfuerzos comercialmente razonables para notificárselo por adelantado, a menos que nos lo impida la ley**…"* (El resaltado no pertenece al original).

Un análisis de las medidas mencionadas, las cuales han sido adoptadas tanto por la SUPEN como por Microsoft para mitigar los riesgos que conlleva el almacenamiento de la información en la Nube, en particular aquellos derivados de la Ley Patriota, hacen pensar a esta Asesoría que en este caso se cuentan con los instrumentos necesarios para continuar utilizando este medio de

almacenamiento, sin que esto conlleve un incumplimiento de la obligación establecida en el artículo 67 de la Ley de Protección al Trabajador, en particular para la información o documentación que le sea suministrada a este órgano de supervisión, y que se refiera a inversiones de un ente regulado por la SUPEN que aún no haya sido divulgada oficialmente en el mercado; así como de la información registrada en las cuentas individuales de los afiliados.

Finalmente, no debe perderse de vista que la naturaleza y trascendencia de los temas que motivaron el dictado de la Ley Patriota, resultan fundamentales no sólo para los Estados Unidos, sino también para un país como el nuestro, que no sólo ha reforzado su legislación interna en materia de lucha contra el terrorismo y el narcotráfico, sino que ha apoyado diferentes esfuerzos relacionados con la cooperación internacional en la materia. Esto hace pensar que ante una solicitud de información formulada por los canales diplomáticos correspondientes, le corresponda a este órgano brindar la colaboración requerida.

## IV. Conclusiones

Del análisis anterior se concluye lo siguiente:

a. Por disposición legal, la SUPEN está obligada a guardar estricta confidencialidad respecto de la información o documentación que le sea suministrada, y que se refiera a inversiones de un ente regulado por la SUPEN que aún no haya sido divulgada oficialmente en el mercado; así como de la información registrada en las cuentas individuales de los afiliados.
b. Esta obligación resulta aplicable a SUPEN no importa si la información confidencial se encuentra almacenada en sus servidores, o en la Nube.
c. Como una excepción a esta obligación, la legislación nacional establece que la SUPEN debe suministrar la información confidencial que le sea requerida en virtud de lo dispuesto en la Ley, o por autoridad judicial competente. Media en este caso un interés superior, que justifica que las prohibiciones contenidas en la Ley en esta materia cedan frente al juez, el cual puede solicitar la información que requiera en el ejercicio de sus potestades y competencias.
d. Lo dispuesto en la sección 203 y 215 de la Ley Patriota sí pueden implicar un riesgo para la información que SUPEN almacena en la Nube, pues es lo cierto que Microsoft se encuentra sujeta a dicha Ley y, por tanto, a las disposiciones sobre acceso a archivos y otros ítems que ésta contiene.
e. La Ley Patriota no se aparta de lo indicado por la legislación y jurisprudencia administrativa costarricense a que se hizo referencia en el punto uno de este dictamen, pues sujeta la solicitud de información a la participación de una autoridad judicial, y siempre en el marco de una investigación realizada en relación con temas de terrorismo internacional o actividades de inteligencia clandestinas. No obstante lo anterior, es claro que se trata de una autoridad judicial extranjera.
f. No obstante lo anterior, y considerando que los riesgos se pueden disminuir, nunca eliminarse completamente, la Superintendencia de Pensiones ha tomado una serie de

medidas para mitigar los posibles riesgos que conlleva el almacenamiento de información en la Nube, a saber:

i. Ha suscrito diferentes acuerdos de servicio con la empresa Microsoft, ello con la finalidad de definir claramente los responsables de atender las eventualidades que se presenten.
ii. Adquirió el certificado SSL con el protocolo HTTPS, lo anterior con la finalidad que los datos que se encuentran en la "Nube" se transmitan encriptados y con ello se pueda dar garantía que el sitio es seguro.
iii. Requiere la autenticación del usuario, para ello uno de los métodos implementados es el uso de certificado digital (firma digital).

g. En este contexto, es importante tener presente que los centros de datos de la empresa Microsoft, los cuales se encuentran geográficamente dispersos, cumplen con los estándares del sector en materia de seguridad y confiabilidad, con la norma ISO/IEC 27001:2005.
h. En relación con la encriptación, y a propósito de lo señalado en el numeral d) de la sección 501 de la Ley de Vigilancia de Inteligencia Extranjera, según fue reformada por la Ley Patriota, en el cual se indica: *Ninguna persona deberá revelar a cualquier otra persona (excepto las personas necesarias para producir las cosas tangibles en esta sección) que el FBI ha solicitado u obtenido información tangible bajo esta sección*, es de prever que en caso de requerirse el acceso a información almacenada por la SUPEN en la Nube, deba recurrirse a este órgano, no sólo para conocer la naturaleza de dicha información, pues Microsoft no cuenta con ese grado de detalle, sino también para que, si es del caso, se colabore proporcionando la clave necesaria para que ésta pueda ser analizada.
i. En este sentido, y desde el punto de vista contractual, SUPEN y Microsoft cuentan con reglas claras a aplicar en caso de que a la segunda le sea requerida información en virtud de lo dispuesto en la Ley Patriota. Claramente en dicho instrumento se indica que: "C*ada una de las partes podrá revelar la Información Confidencial de la otra* ***si se le exige que cumpla una orden judicial*** *o* ***cualquier petición gubernamental que tenga fuerza de ley****. Antes de hacerlo, cada una de las partes debe buscar el nivel más alto de protección disponible y, cuando sea posible, notificar con suficiente anterioridad a la otra para que tenga una oportunidad razonable de buscar una orden de protección judicial..."* (El resaltado no pertenece al original). Nótese que la solicitud siempre se sujeta a la Ley, e implica que sea formulada por funcionarios judiciales investidos para tal efecto.
j. Por otro lado, este contrato se ve complementado por el compromiso público que Microsoft hace constar en el sitio http://www.windowsazure.com/es-es/support/trust-center/faq/, cuyo texto es el siguiente: *"...* ***¿Qué sucede si terceros le solicitan mis datos de cliente a Microsoft con fines legales u otros propósitos? ¿Qué hará Microsoft si recibe una citación en la que se solicitan datos de clientes?*** *Microsoft cree que sus clientes deben controlar su propia información, esté almacenada de forma local o en un servicio en la nube. En consecuencia,* ***no revelaremos los datos de los clientes a terceros*** *(ni siquiera a una autoridad judicial, otra entidad gubernamental o litigante civil)* ***salvo que usted lo indique o por imperativo legal****. Si terceras partes se pusiesen en contacto con nosotros solicitando datos de clientes,* ***les indicaríamos que se los solicitasen directamente a ellos****. A tal fin, les podríamos proporcionar*

*información de contacto básica.* ***Si nos viésemos obligados a revelar sus datos de cliente a terceros, emplearíamos todos los esfuerzos comercialmente razonables para notificárselo por adelantado, a menos que nos lo impida la ley****…"* (El resaltado no pertenece al original).

k. Las medidas descritas, las cuales han sido adoptadas tanto por la SUPEN como por Microsoft para mitigar los riesgos que conlleva el almacenamiento de la información en la Nube, en particular aquellos derivados de la Ley Patriota, hacen pensar a esta Asesoría que en este caso se cuentan con los instrumentos necesarios para continuar utilizando este medio de almacenamiento, sin que esto conlleve un incumplimiento de la obligación establecida en el artículo 67 de la Ley de Protección al Trabajador, en particular para la información o documentación que le sea suministrada a este órgano de supervisión, y se refiera a inversiones de un ente regulado por la SUPEN que aún no haya sido divulgada oficialmente en el mercado; así como de la información registrada en las cuentas individuales de los afiliados.

l. No debe perderse de vista, además, que la naturaleza y trascendencia de los temas que motivaron el dictado de la Ley Patriota, resultan fundamentales no sólo para los Estados Unidos, sino también para un país como el nuestro, que no sólo ha reforzado su legislación interna en materia de lucha contra el terrorismo y el narcotráfico, sino que ha apoyado diferentes esfuerzos relacionados con la cooperación internacional en la materia. Esto hace pensar que ante una solicitud de información formulada por los canales diplomáticos correspondientes, le corresponda a este órgano brindar la colaboración requerida.

Cordialmente,

Elaborado por: Yorleny Avendaño Vega

Revisado por: Jenory Díaz Molina

Aprobado por: Nelly Vargas Hernández

***División Asesoría Jurídica***