INFORME TECNICO N° 3

RIESGOS DEL CLOUD COMPUTING

ASPECTOS LEGALES Y TÉCNICOS

Comisión de Estudios sobre Sistemas de Registro, su integridad y autenticidad documental

Contenido

I Que es el concepto computación en la nube (cloud computing)

Introducción

Del mismo modo que la incorporación de la computadora de escritorio significó para los sectores de administración, una revolución en las formas de realizar los trabajos, lo mismo aconteció con el advenimiento de Internet y la apertura de esta herramienta para todas las personas.
Como todos sabemos esto significo la posibilidad de compartir información con mucha gente.
Se comparte mucha información con tantas personas que es común perder de vista dos cuestiones fundamentales:

1- Quienes tienen acceso a nuestros datos.
2- A que datos le estamos dando acceso.

En la actualidad la penetración de internet, el desarrollo de algunos programas y aplicaciones, la popularidad obtenida por algunos de estos, nos colocan frente a situaciones muy complejas.
Elegir pertenecer al grupo de usuarios de determinados programas o quedar al margen de su utilización, sin poder basarnos para tomar esta decisión en criterios de resguardo de nuestras informaciones personales. Esto es así porque los programas a los que hacemos referencias trabajan con la mecánica de que entreguemos información personal, para pertenecer al grupo de usuarios del mismo y entonces estar conectados.

Ahora bien, a quien le estamos entregando nuestra información?

La mayoría de nosotros, cuando aceptamos la utilización de un programa de aplicación general estamos aceptando trabajar con una empresa de la que probablemente conozcamos su nombre comercial, o el nombre comercial de su aplicación más popular.
Pero no sabemos la razón social, la forma legal que aplica en el territorio nacional, muchas veces desconocemos si existe sede social en nuestro país, si hay un representante legal en nuestro territorio, etc.

El concepto de Cloud Computing o Nube es la posibilidad de tener diferentes equipos de computación, trabajando en forma simultánea, compartiendo información, independientemente de la localización geográfica de los mismos.

De este modo toda la información que los usuarios hayan cargado en algún lugar a través de un servicio de web de computación, estará viajando por diferentes lugares geográficos, hasta estacionarse en algún otro lugar geográfico, sin que el dueño de la información tenga el debido conocimiento de donde están sus datos.

Para que una nube trabaje como tal se necesitan equipos de computación que alojen datos, equipos de comunicación, servicios de comunicación y los equipos de los usuarios propietarios de estos datos, que probablemente sin saberlo pasan a ser parte de esta nube, dado que sus computadores se transforman en las fuentes de ingresos de los datos en cuestión. Estos equipos se utilizaran para generar, consultar o modificar estos datos.

El cloud computing no es exclusivo para la utilización de usuarios individuales, y sus datos personales, sino que el el cloud computing es una forma de trabajar que por lo tanto se pone a disposición de las empresas o cualquier otro tipo de organización.

Es entendible que un sistema de estas características genera importantes ahorros de costos.
Lo que cuestionamos es que un sistema basado en estas características vulnera principios legales, sobre todo los que hacen a las garantías indiviuales, a la defensa de la privacidad de los datos, a los derechos de consumidor.

El cloud computing puede ofrecernos todas las funcionalidades que nos brinde un sistema de computación integrado, ofertándolo como servicios inconexos. La suma de esos servicios inconexos termina otorgándonos las funcionalidades de un sistema de computación integrado.

La evaluación que haga un usuario personal acerca de utilizar servicios en la nube, no debe ser la misma que la que haga un usuario organización puesto que este último está representando a un número mayor de personas individuales. También por esto es que las organizaciones están obligadas a cumplir con normativas y regulaciones legales y de entes de contralor.
Cuando una organización decide contratar un servicio en la nube deberá entonces verificar que ese servicio cumpla con los requisitos legales que para ese servicio se exijan en el país.

Que tipo de recaudos debe tener la organización que decide operar mediantes servicios en la nube?
Que tipo de contratos son aplicables? Como sabemos si estamos actuando cumpliendo los requisitos legales?
Que tipo de controles o de seguridades le debemos exigir al prestador de servicios respecto a las restricciones de acceso a la información, o a la ubicación de los datos jurisdiccionalmente hablando?

Todas estas cuestiones desarrollaremos en el presente trabajo.

Definición

Definiremos entonces no desde el punto de vista técnico sino desde el punto de vista de estudio simplificado que damos a esta primer etapa del trabajo que todo Sistema de Registros (incluido sus documentos digitalizados o digitales y la base de datos del sistema) esta en un cloud si los mismos se acceden desde un dispositivo informático que no tiene en su sistema de almacenamiento interno dicha información.

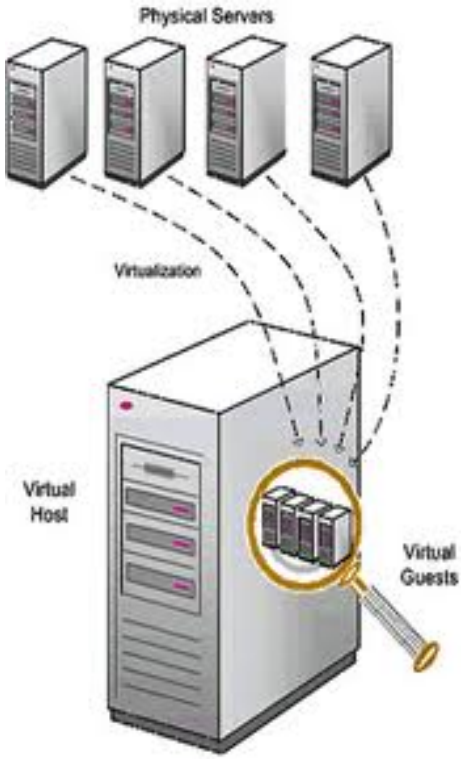
II Diferencias ente la nube privada y pública (private and public cloud)

Las entidades que poseen sistemas soportados en una/s computadora/s propia de alto nivel de procesamiento de datos llamadas servidor/es y a la que acceden sus empelados y terceras partes autorizadas trabajan en un la nube privada.

Si por el contrario si contratan espacios (hosteo) en servidores de empresas que prestan esos servicios y en ellos depositan sus sistemas de registros y documentación digital y digitalizada para que accedan sus empleados y terceras partes autorizadas, trabajan sobre un cloud privado.

Esta definición elemental era la que se correspondía en la década del 80 del siglo pasado, pero a medida que el avance tecnológico comienza a crecer a bases exponenciales: mayor velocidad, mayor capacidad de procesamientos múltiples y complejos, menor costos de almacenamiento, mayor espacio de almacenamiento, menos tamaño en los equipos, comienza a complicarse.

Desde hace unos años comenzaron fabricarse servidores que pueden auto dividirse mediante software en varios servidores. Este proceso se llama virtualización, el grafico a continuación muestra lo que se explica en estas líneas



Mediante la virtualización una misma empresa puede asignarle a cada sector servidores independientes para trabajar. En tanto que un proveedor de hosting hará lo mismo con sus diferentes clientes (entidades). Con lo cual en un mismo servidor físico pueden convivir en una

nube privada Logística, Finanzas, Comercialización, etc., como si cada uno tuviera un servidor propio y en la nube publica entidades privadas y publicas, paginas Web, repositorios de películas y música que se comparte, etc.

Como un centro de procesamiento de datos es caro puesto que precisa infraestructura especial en el edificio, el cableado, la refrigeración y la seguridad, la virtualización mejoro sustancialmente los costos permitiendo servicios a gran escala. Es más económico para las empresas solicitar un servicio de hosteo que tener su propio centro de procesamiento de datos. En otro casos el respaldo de la información procesada que por seguridad no puede estar en el mismo espacio físico en un radio inferior al desastre mayor que pueda afectar esa zona (no es la misma distancia si hay estaciones de servicios, depósitos de material inflamable, zona inundable, etc.) no justifica el armado de un centro de procesamiento de datos y es mas económico contratar el servicio de hosteo.

Estamos en condiciones de definir entonces las redes públicas y privadas según las siguientes variantes:

1. Dentro del mismo centro de cómputos del ente conectados por red propia (LAN)
2. Dentro de los distintos centros de cómputos del ente conectados por red propia (LAN)
3. En oficinas dentro del mismo edificio conectados por red propia (LAN)
4. En oficinas (fuera del centro de cómputos) dentro de diferentes edificios conectados por una red propia (LAN)
5. Permitiendo el acceso remoto de los usuarios desde otros punto fuera de la empresa mediante red pública (WEB)
6. En servidores de terceros contratados para alojar la información (hosteo) al que se conecta por red propia (LAN) o por conexión pública (WAN)

Las opciones 1 a 4 conforman una nube privada

La opción 5 es un uso público de la nube privada

La opción 6 conforma una nube pública

Más adelante se explica que por motivos de seguridad la opción 6 no puede aceptarse sino bajo condiciones muy específicas.

III Los aspectos legales que afectan a la nube pública y privada

La normativa vigente obliga a los entes a que los Sistemas de Registros estén en la jurisdicción donde el ente tiene su domicilio legal declarado ante la autoridad de registro.

En términos prácticos los centros de procesamiento de datos de entidades que se encuadran dentro del Art. 61 de la Ley de Sociedades Comerciales no pueden estar en otra jurisdicción que no sea la del domicilio de la Sociedad.

Por otra parte las entidades que no se encuadran en este artículo pueden tener su centro de procesamiento de datos en cualquier lugar del mundo mientras los libros rubricados se encuentren en la jurisdicción de la sede social

Creemos que esta situación no es la adecuada si se trata de tener un Sistema de Registros que asegure la integridad ya autenticidad de los datos que lo conforman, debiendo exigirse a todo los entes que procesan informáticamente parcialmente la información de su Sistema de Registros cumplir con las mismas normas. Esto se basa en que la integridad y autenticidad puede ser alterada en el procesamiento por lo cual lo que se vuelca a un libro rubricado no necesariamente es autentico e integro.

En los modelos de nube privada resulta mas sencillo el cumplimiento del aspecto jurisdiccional, aunque no siempre se cumpla pero en la nube publica donde hay una cadena de intermediarios de los proveedores de hosteo en lo servicios para PyMEs verificar este cumplimiento es mas complejo.

Creemos importante que la Ley se adapte a las necesidades de los entes de contralor pero adecuándose al mercado. De hecho el BCRA le permite a Bancos extranjeros que su centro de procesamiento este fuera del país pero con un acuerdo de permiso de acceso físico al sistema de Procesamiento de datos en el lugar donde se encuentra geográficamente. Para esto es necesario regular los contratos de hosteo y/o tratamiento (cada vez hay más software de Sistema de Registros en la nube) de forma tal que se deje en ellos:

- La identificación fehaciente de las entidades prestadoras del servicio (intermediarios y prestador inicial)
- Responsabilidades de las partes intervinientes
- Nivel de servicio a prestar: detalle, horarios, nombre de los contactos, forma de contacto, horario de contacto
- La información de la ubicación física del Sistema de Registro y su copias de respaldo,
- Medidas de seguridad en el servicio
- Autorización fehaciente en el acceso físico a los Sistemas de Registro y sus copias de respaldo y procedimiento de acceso acordado de acuerdo con normativa vigente
- Detalle del perfil del personal autorizado al tratamiento y de sus responsabilidades
- Acuerdo del tipo de sanciones en caso de incumpliendo
- Para cumplir la Jurisdicion se pude hacer mediante un back up para recuperación y un copia espejo del tipo continuidad de negocios, es decir que contenga:
  - El Sistema de Procesamiento de los Registros en su última versión y el de
  - versiones discontinuadas
  - Las transacciones diarias que generaron registros

- Los logs (su nombre de usuario por el que accede) de los usuarios y
- administradores del Sistema Operativos, del Sistema de Registros y de la Base
- de Datos y sus Altas, Bajas y Modificaciones (ABM)
- El historial acumulado por ejercicio contable de los logs de los usuarios y
- administradores con el detalle de proceso A,B,M,C (C=consulta)
- La Base de Datos completa
- Opcional pero recomendable: copia de todos los mail recibidos y enviados, acumulados por ejercicio y copiados diariamente

IV Los aspectos técnicos que afectan la seguridad de los sistemas de registros informatizados

Son varios los elementos que generan riesgos s al información que conforma el Sistema de Registros y se resumen en:

1. La ubicación física y lógica de la información
2. El canal de comunicación
3. El acceso a la información
4. La infraestructura en la que se alojan los servidores

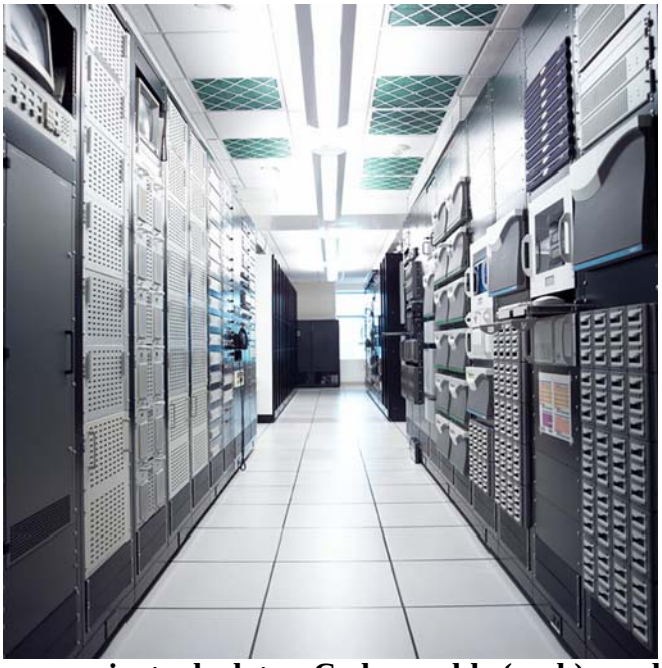
Los riesgos relacionados con la ubicación de la información

La virtualización de los servidores es lo que potencia el concepto cloud que simplificamos en le capitulo anterior. Si recordamos que la virtualización de servidores es un proceso lógico que permite que lo que antes físicamente estuviera en un servidor fuera reemplazado por servidores que permiten dividirse a sí mismo como varios servidores independientes pero físicamente es el mismo computador, es decir que si miramos la configuración del servidor físico, veremos que está dividido en varios servidores lógicos que operan en forma independiente unos de otros pero que comparten el sistema operativo que les permite esta división. Entonces podemos entender que a partir de esos procesamientos lógicos también se facilita la optimización de los espacios en el disco y los tiempos de proceso, de los servidores físicos que forman el centro de procesamiento de datos y que se los interconecta mediante una red.

Allí comienza el primer problema para asegurar la información y es saber dónde está. El por qué merece una explicación muy simple: esos servidores optimizan los recursos de procesamiento según la cantidad de usuarios e información que se está procesando y lo transmiten a otro servidor virtual (no necesariamente en el mismo servidor físico) que en ese

momento tiene más disponibilidad de procesamiento y eso aumenta la velocidad de los procesos. Pero estas trasmisiones entre servidores son continuas, automáticas, y sin recursos de software que permita monitorear a donde se envió la información o el Sistema de Registros, no es posible saber en qué servidor lógico y físico está.

Cual es la información que debemos saber donde esta: el sistema de Registro y sus bases de datos y los documentos sean estos digitales o se hayan digitalizado



Vista de un centro de procesamiento de datos. Cada mueble (rack) puede albergan hasta 45 servidores u otros elementos de procesamiento

El canal de comunicación

Sea una red Lan (privada) o Wan (publica) la conectividad será una de las siguientes o la combinación de ellas:

- cable telefónico: servicio de internet (WAN) de las empresas telefónicas de Argentina para hogares de todo el país y empresas fuera de CABA,
- cable coaxial: servicio de empresas de cable de CABA y parte del Gran Buenos Aires y ciudades importantes del resto del país
- cable coaxial dentro del cableado de la empresa (LAN)
- mezcla de cable coaxial y fibra (son redes configuradas con un troncal de fibra pero a los usuarios se llega con cable coaxial.): servicios hogareños y a empresas PyMEs de internet (WAN) de fibra en CABA y parte del Gran Buenos Aires y algunos servicios en el interior del país.

- fibra óptica (WAN) servicios de conectividad empresarial en CABA y grandes ciudades del país.
- fibra óptica (LAN) cableado de la empresa
- inalámbrica microonda terrestre (LAN o WAN) servicios centrado en CABA, Gran Buenos Aires y grandes ciudades del interior del país.
- inalámbrica microonda satelital (LAN)
- acceso inalámbricos a todas las redes (LAN)

Sean estas privadas (LAN) o públicas (WAN), las redes pueden ser accedidas por terceros no autorizados:

- de forma física, es decir enganchándose con un corte en el cable de red
- en forma remota por la propia exudación de lo que las redes transmiten, siendo el riesgo mayor para el cable telefónico, le sigue el coaxial y finalmente la fibra óptica
- con tecnología más sofisticada con el ingreso remoto a esa transmisión sea en red de cable o inalámbrica

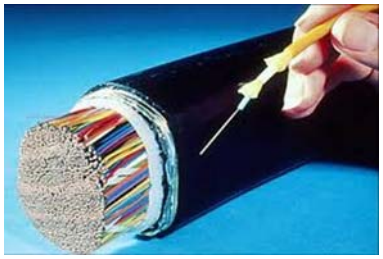
Los puntos más vulnerables de las redes por el fácil acceso que permiten físicamente son los de interconexión en su tendido. La transmisión inalámbrica en todas sus formas: ondas de radio, microondas terrestres y satelitales, infrarroja, resultan ser las más vulnerables de todas las formas de comunicación.

Por eso la seguridad lógica y física en las redes es fundamental. La forma de transmitir la información es la clave para asegurar la información la cual debe ser con encriptación de alto nivel, protocolos de comunicación seguros, filtros y administradores de acceso restringido dentro del cableado de la red y en los puntos de acceso tanto físicos como lógicos. La configuración de la red debe ser, documentada en detalle (es decir indicando quien, en que horarios, en que forma, ante que situaciones, a que tiene acceso) con su correspondiente evaluación de riesgos y aprobada por la Dirección del ente.

Los riegos de la red deben ser evaluados en forma continua en función al avance tecnológico y a los eventos de seguridad que se denuncian mundialmente, para realizar las modificaciones necesarias para mantener los niveles de riesgo en su nivel más bajo.

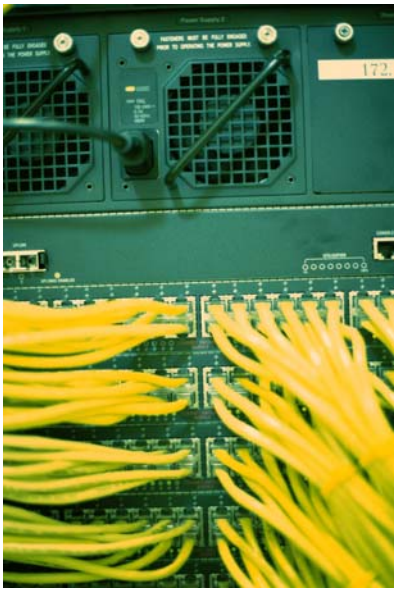
Por otra parte el acceso remoto a los sistemas que se hace mediante redes WAN o LAN de microonda terrestre o satelital o sistemas inalámbricos del tipo personal (WIFI, Bluetooth, etc.) debe ser bajo procedimientos de validación (autorizar equipos predeterminados y sus usuarios) para evitar intromisiones que afecten la seguridad de los Sistemas de Registros y la base de datos, como se explica más adelante.

A la izquierda un satélite de comunicación de datos y a la derecha una microonda



A la izquierda cable coaxial donde la línea es de ida y vuelta y a la derecha una fibra óptica donde cada pelo es un canal de comunicación independiente de ida o vuelta

Cable telefónico cada línea es un canal de comunicación de ida o vuelta



Cada Cable comunica al servidor con otro servidor o periférico que lo administra

Los riegos relacionados con el acceso a la información

Como analizamos que no podíamos saber dónde estaba la información sin software adecuado, determinamos donde se centran los problemas para asegurar la información: en que los dispositivos que filtran las intromisiones (firewalls) y permiten configurar los accesos de los usuarios trabajan sobre un solo servidor (swichers). Lo habitual en un centro de cómputos es que los firewalls y los switchers se conecten a cada servidor o estén incluidos en el propio servidor (servidores blade). La configuración de estos dispositivos de seguridad se realiza en forma individual para cada servidor, lo cual dificulta aplicar políticas de acceso según el tipo de información que el servidor procesa si la información está migrando en forma continua entre distintos servidores físicos.

Cabe aclaran que si bien el espacio de hosteo puede para seguridad estar encriptado esta barrera de seguridad no es suficiente para impedir las intromisiones de terceros (hackeos), por lo cual siempre son necesarias las barreras antes mencionadas

Estos ejemplos pueden clarificar el tema:

1. El ente define que a internet puede entrar todo el personal y los terceros que realizan consultoría. La política de acceso permite que todo el personal y esos consultores tengan primero acceso al servidor que presta el servicio de conexión a internet y luego a internet.
2. A los Sistemas de Registros puede acceder el personal de las áreas que hacen tratamientos (alta, baja modificación consulta y proceso) de operaciones contables, los auditores y el síndico. La política de acceso seria que esas personas primero tengan acceso al servidor y luego al Sistema de Registros con accesos limitados según la tarea que realizan.

Si los servidores no fueran virtuales, la configuración de los swichers seria con una política amplia en el primer caso y restringida en el segundo. Restringir el acceso al servidor es parte de las políticas de seguridad de la información de cualquier Sistemas de Registros conocidos como ERP (Enterprise Resource Planning) de alto nivel, como SAP; y una necesidad imperiosa no exigida en otros ERP; algunos de estos últimos con fácil acceso a las bases de datos para procesar la información por afuera (argumento que resaltan en la venta). Podemos imaginar que puede pasar con la información del Sistema de Registros si cualquiera puede acceder al servidor donde está la base de datos. Tener acceso al servidor es la primera barrera de control de acceso y es fundamental; porque la mayoría del software que no es de primer nivel, el acceso a su base de datos por fuera del Sistema de Registros es muy fácil si se puede acceder al servidor. Ni hablar si los ERP de primera línea fueron mal configurados y sus bases de datos quedaron accesibles, algo que es mucho más común de lo que parece a simple vista (la AFIP es un ejemplo de este tipo de configuración incorrecta). Cabe aclara que el riesgo antes descripto de bases de datos que pueden ser accedidas por fuera del Sistema de Registros es un riesgo en sí mismo sin importar si los que tiene acceso al servidor son el personal asignado al registro de los procesos contables, los auditores y el síndico; esto debería ser normado como prohibido en una modificación del Art.280 de la Resolución IGJ 7/2005.

Restringir el acceso al servidor no puede hacerse con servidores virtuales a menos que se cuente con software que cumpla las funciones de firewall y swichers. Este software ha sido desarrollado pero no esta implantado en todos los centros de procesamiento de datos virtualizados. Sin embargo antes de la existencia de la herramienta y aun hoy hay empresas procesando sin estas herramientas con lo cual la información del Sistema de Registro pudo haber sufrido serios incidentes de seguridad, lo cual no la hace confiable

La infraestructura en la que se alojan los servidores

Los riesgos que enfrenta el edificio donde se aloje el centro de procesamiento de datos que contiene a los servidores en uso por el Sistemas de Registro y sus copias de resguardo debe tener en cuenta desde su ubicación geográfica hasta su diseño y operación para lo cual deberá tomar las medidas necesarias para mitigar estos riesgos mediante:

- Sistemas redundantes de energía eléctricas provistas por las centrales publicas (pertenecer a dos centrales diferentes que se swichean automáticamente)
- Elegir zonas con baja posibilidad de inundaciones, incendios, robos, terremotos, etc.
- Construcción en materiales seguros con accesos restringido en áreas anidadas

En el funcionamiento del centro de procesamiento de datos debe contemplar

- Implementar medidas de seguridad documentadas y hacer las pruebas necesaria para actuar en caso de incendio o inundación como así también ante cualquier incidente que impida el funcionamiento del centro de procesamiento de datos

Respecto a la infraestructura necesaria en el ambiente en que se instalen el equipamiento de computación y comunicaciones se debe tener elementos de lata calidad (homologados) y con cumplimiento de buenas practicas como son:

- Sistema propio que le de autonomía ante cortes de suministro eléctrico de las centrales proveedoras y hasta que se restablezca.
- Materiales ignifugos
- Piso técnico flotante y techo técnico que permitan el tenido de cables y cañerías en forma asilada y con acceso a reparaciones limpias (sin rotura de mampostería).
- Cableado de red y teléfono en materiales homologados y con redundancia (que permita ante la caída de uno tomar otra vía de comunicación).
- Cableado eléctrico homologado con tableros seguros
- Instalación de alarmas, control de temperatura y humedad con avisos.
- Facilidad de acceso mediante puertas amplias para el ingreso de equipamiento
- Airea acondicionado que mantenga temperatura y humedad estables
- Cerraduras con controles biométricos
- Cámaras de seguridad vigiladas y con registro para control de evento de seguridad (grabación)
- Detectores de movimiento con registro de control de eventos de seguridad mediante avisos

V Como asegurar la integridad y la disponibilidad en la nube privada

Existen dos posibilidades muy claras y que se diferencian entre sí en función a los recursos tecnológicos que se dispongan:

I. Se puede virtualizar si se cuenta con software que permita:
   1. configurar las características del servidor virtual como dedicado (es decir como exclusivo) cada vez que se migre el Sistema de Registros y su Base de Datos
   2. restringir los accesos a la configuración de seguridad requerida por ley para estos Sistemas y Datos
   3. localizar físicamente en que servidor está dicha información no solamente en forma lógica.

II. No se puede virtualizar si no se cuenta con la tecnología de software antes indicada. En este caso los Sistemas de Registro y su base de datos deberán:
   1. Alojarse en un servidor físico dedicado, es decir que siempre sea en forma exclusiva para esta información.

2. Cualquier migración deberá realizarse con intervención del área de puesta en producción de los sistemas y la base de datos con previa configuración de los servidores bajo la seguridad requerida.

III. En ambos casos la red LAN deberá tener la configuración de seguridad necesaria para evitar acceso de terceros y transmitir los paquetes de información encriptados. Si la LAN une espacios fuera del edificio o el cableado esta accesible a terceros la seguridad deberá ser sobre el área física de la red también.

IV. En ambos casos los accesos remotos vía WEB (Red WAN) o vía conexión inalámbrica (Red WAN o LAN) o inalámbricas personales (Red LAN) deberá configurase el servidor de forma tal que ante la petición de conexión verifique con llamado de retorno la identidad del peticionante antes de autorizar la conexión, esto es que el acceso sea sobre líneas y computadoras previamente reconocidas como de propiedad asignada al usuario además de la identificación del mismo.

V. En todos los casos los controles de acceso físico al centro de cómputos o donde se encuentre los servidores, debe incluir la imposibilidad de acceder con dispositivos de almacenamiento y de comunicaciones móviles (pen drive, teléfonos, reproductores de mp3, tablets, computadoras personales, etc.). Restringir el acceso a las personas autorizadas (internos y externos) y tener firmados convenios de confidencialidad y régimen sancionatorio. Se deberán documentar y reportar al Directorio los eventos de seguridad al igual que la documentación e investigación posterior.

VI Como asegurar la integridad y la disponibilidad en la nube publica

En este caso hay que determinar claramente en el contrato de servicios:

I. El lugar físico donde están los servidores:
   1. En el territorio de la República Argentina denunciando las jurisdicciones y teniendo un representante en la jurisdicción sede del ente lo cual deberá estar claramente especificado en el contrato que permita la atención de los entes clientes en cualquier momento que deban acceder a su Sistema de Registros en forma física al igual que la localización de los back up propios del prestador del servicio.
   2. Si los servidores están fuera del territorio de la República Argentina, el proveedor deberá tener un representación en el país a cargo de personas con formación profesional del Derecho Contable que les permita evaluar la situación de riesgo de los Sistema de Registros y de los back up propios del proveedor del servicio que contengan el sistema de registros, donde están alojados, el cumplimento de restricciones por la Ley 25.326 de Protección de Datos Personales y la disposición de atención a los entes clientes ante cualquier requerimiento. Esta representación podría ser dada directamente a cualquier profesional matriculado, con la formación antes especificadas y pleno acceso tecnológico a la monitorización del servidor donde se encuentra el Sistema de Registros y las back up propios del prestador del servicio y los reportes necesarios para el control. Cabe aclarar que los back ups propios del prestador de servicios son datos cuya propiedad no le corresponde y por lo tanto deben

estar bajo el control de quien ejerza la representación en la jurisdicción del ente.

II. Las medidas de seguridad en la configuración de los accesos físicos y lógicos a la Red según lo exigido en los puntos III y IV de las condiciones del prívate cloud

III. Los controles de acceso a los servidores los cuales deberán cumplir con los puntos I y II de la prívate cloud.

IV. Los controles de acceso físico al centro de cómputos que debe incluir la imposibilidad de acceder a los servidores con dispositivos de almacenamiento y de comunicaciones móviles (pen drive, teléfonos, reproductores de mp3, tablets, computadoras personales, etc.) y el listado de las personas autorizadas al igual que los convenios de confidencialidad y régimen sancionatorio.

V. Los controles de acceso físico y lógico a los swichers y firewalls y el listado de las personas autorizadas al igual que los convenios de confidencialidad y régimen sancionatorio.

VI. La responsabilidad solidaria del proveedor del servicio ante los eventos de seguridad y el reporte sistemático de los mismos al ente contratante, al igual que la documentación e investigación posterior.

VII Conclusiones

Las tecnologías avanzan en el sentido del public cloud y en menor medida al private debido al abaratamiento de costos de infraestructura; esto se debe a que en gran escala la operatividad de un centro de cómputos de primer nivel en cumplimento de normas internacionales de seguridad y disponibilidad (Word Class) es más económico. Por eso debemos adecuar la normativa a esta tendencia sin perder el objetivo de que los Sistemas de Registros sean seguros: íntegros, disponibles y con la confidencialidad legal exigida.

Como asesores de empresas deberemos poner a nuestros clientes al tanto del cumplimiento de estas buenas practicas aun no legisladas para evitar incidentes de seguridad que afecten su información y por lo tanto la toma de decisiones, el cumplimento legal y hasta la continuidad del negocio.

En cuanto a las empresas que hoy no operan bajo estas condiciones debería realizarse un análisis forense antes de dar como válida la información de su Sistema de Registros. Es decir que se deberán analizar de los eventos de seguridad para determinar los incidentes de seguridad que puedan verificarse mediante la revisión del sistema operativo, la base de datos y el Sistema de Registros como así también cualquier incidente en el Centro de Cómputos o en los lugares donde se encuentren los servidores. Ante esta situación deberá considerarse como posible incidente de seguridad todo evento que genere modificaciones a los datos, copia de datos desde y hacia el servidor, accesos fuera de horario, reiterados intentos de accesos denegados, información borrada, accesos a la base de datos y toda otra actividad que pudiera haber alterado la integridad de los registros.

VIII Bibliografía

- IRAM/ISO/IEC 27002:2005 Código de práctica para la gestión de la seguridad de la información, 2008
- IRAM/ISO/IEC 27001:2005 Sistemas de gestión de seguridad de la información (SGSI) Requisitos, 2007
- MERCOSUR/ISO/IEC 27005:2008Gestión del riesgo de seguridad en la información, 2008
- CISCO Data Center Design & Deployment Seminar 2011, Buenos Aires Argentina 2 y 3 de mayo Data Center Virtual de CISCO.
- Magic Quadrant for Secure Web Gateway Gartner RAS Core Research Note G00212739, Laurence Orans, Peter Firstbrook, 25 May 2011,V3 RA1 05272012
- Resolución IGJ 7/2005
- Seguridad y Cloud Computing, hacia un cambio de paradigma Rodrigo Parreira, CEO de Logicalis para el Cono Sur - Logicalis Now marzo 2011
- La Nube plantea nuevos desafíos de lnfraestructura por Lujan Scarpinelli Diario La Nación octubre 16 de 2011

IX. Autores

Este Informe fue preparado por un grupo de trabajo integrado por los Doctores:

Iglesias, Silvia G.
Vera, Alejandro M.

Versión revisada y actualizada por los autores del Capítulo del mismo nombre del Libro Derecho Contable Aplicado ERREPAR

Las autoridades de la ***Comisión de Estudios sobre Sistemas de Registro, su integridad y autenticidad documental***, son los Doctores

Iglesias, Silvia G.- *Presidente*
Braga, Graciela I. - *Vicepresidente*
Valsangiacomo, Guillermo F. - *Consejero Coordinador*

El trabajo fue aprobado en la reunión plenaria del 10 de junio de 2014 por los miembros presentes en la ocasión:

Avalos,Gustavo
Diaz, Oscar
Maggi, Marta

Mazzitelli, Esteban C.
Osso, Maria C.
Pavicich, María C.
Pavichevich, Gladys
Vera, Alejandro M.

Buenos Aires, 10 Junio de 2014.