Buenas Prácticas para el uso de Servicios *Cloud Computing* al interior de la Administración del Estado.

Versión 2
Santiago, 19 de Febrero de 2018
División de Gobierno Digital

Índice

Introducción

1. Preámbulo

La División de Gobierno Digital, en su rol de coordinar, asesorar y apoyar en el uso estratégico de tecnologías digitales, datos e información pública para mejorar la gestión de los órganos de la Administración del Estado y la entrega de servicios, y entendiendo la importancia de la adopción de tecnologías que promuevan la eficacia, eficiencia e innovación, se ve en la necesidad de entregar pautas y lineamientos generales a los órganos de la Administración del Estado para la evaluación e implementación de servicios en la nube (también llamados servicios "*cloud*") para los casos en que este tipo de servicios sean:

1. Adecuados al propósito que se requiera cumplir.
2. Cuando sean eficientes en el sentido económico.
3. Cuando los riesgos sobre la información y los activos de información sean adecuadamente gestionados.

Es importante reconocer que los ciudadanos esperan que los servicios provistos por los órganos de la Administración del Estado respondan a sus necesidades y estén disponibles cuándo y dónde ellos los necesiten, por lo que se hace necesario el uso efectivo y eficiente de los recursos tecnológicos, incluyendo la adopción y el uso de los servicios *cloud* cuando éstos sean apropiados.

Existen grandes beneficios potenciales en torno al uso de esta tecnología, puesto que su utilización puede implicar importantes ahorros de costos económicos y de tiempo en la gestión de plataformas electrónicas. Además, la computación en nube puede entregar beneficios tales como la escalabilidad, elasticidad, alto rendimiento, resiliencia, ubicuidad y seguridad. La computación en la nube ha revolucionado la forma de entregar servicios y recursos informáticos a los usuarios, mediante un enfoque bajo demanda, y con un alto grado de innovación, dando pie a una transformación de los servicios provistos por el sector público en soluciones ágiles, eficientes y medioambientalmente sustentables.

Por las razones antes mencionadas, la División de Gobierno Digital recomienda, como regla general, la evaluación de este tipo de soluciones tecnológicas al interior de los órganos de la Administración del Estado. Ello atendido a que dicha tecnología impacta positivamente en la forma en que tales órganos ejercen sus funciones, con plena consonancia con los principios de eficacia y eficiencia que considera el artículo 3° de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado.

Además, la División de Gobierno Digital está comprometida con esta recomendación al liderar con el ejemplo, implementando la mayoría de los servicios que presta mediante esta modalidad, generando importantes beneficios en las áreas antes mencionadas.

2. Objetivos

El objetivo de esta guía práctica es dar a conocer los beneficios de la computación en la nube a los organismos de la Administración del Estado, así como también las consideraciones y cuidados principales para su adopción, a través de un documento informativo, de carácter

pedagógico, donde las distintas entidades podrán encontrar los puntos clave respecto de los beneficios, principales usos, potenciales riesgos y resguardos a considerar al momento de contratar servicios en la nube, entre otros.

3. Descripción del Contenido de esta Guía

Este documento está estructurado en dos partes principales. En la primera, se entregan definiciones y conceptos claves para entender de mejor manera la tecnología *cloud*, y en la segunda, se entregan las principales ventajas comparativas de utilizar la nube versus infraestructura tradicional, así como también algunas consideraciones y cuidados fundamentales que se deberían tener presentes al considerar un servicio en esta modalidad.

4. Sobre el presente documento

Este documento no es vinculante para los órganos de la Administración del Estado. No pretende, tampoco, establecer una política de contratación en este tipo de materias. Tales órganos son libres de tomar las decisiones que estimen convenientes en torno a esta materia, en la medida que se adopten dentro de sus competencias y de conformidad al marco legal que las rige.
Este documento sólo pretende entregar antecedentes que permitan la toma de decisiones informadas por parte de tales órganos, adoptando las buenas prácticas que aquí se sugieren.

Definiciones y conceptos claves

La División de Gobierno Digital ha asumido la definición de *Cloud Computing* del NIST (2011)[1]: La computación en la nube es un modelo para habilitar a través de la red acceso ubicuo, conveniente y bajo demanda a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente aprovisionados y liberados con un mínimo esfuerzo de gestión o interacción con el Prestador de Servicio *cloud*.

Los modelos de *Cloud Computing* se componen de cinco características esenciales, tres modelos de servicio y cuatro modelos de implementación, sin perjuicio de que existan más modelos que los descritos a continuación:

Características esenciales de un servicio *Cloud Computing*.

1) **Autoservicio bajo demanda:** El cliente puede contratar sólo los servicios que requiere y cuando los necesite, sin necesidad de mayor interacción con el Prestador de Servicios *cloud*.
2) **Amplio acceso a la Red:** Los servicios quedan disponibles ampliamente acorde a las reglas de acceso que se definan, pudiendo generar recursos compartidos de manera sencilla.

[1] NIST: National Institute of Standards and Technology , United State, Departament of Commerce http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

3) **Recursos Compartidos:** Los recursos tecnológicos del Prestador de Servicio son agrupados para servir a múltiples clientes, siendo asignados y reasignados de forma dinámica y bajo demanda.
4) **Elasticidad:** Las capacidades requeridas se pueden asignar y retirar de forma elástica y a menudo automáticamente, respondiendo de forma flexible a la demanda de recursos de los clientes.
5) **Servicio medido:** Se aprovecha la capacidad de medición en algún punto apropiado del servicio para permitir al cliente consumir sólo lo que necesita.

Modelos de Servicio para *Cloud Computing*.

1) **Infraestructura como Servicio (IaaS)**: Servicios que entregan almacenamiento básico y capacidades de cómputo como servicios estandarizados en la red. Servidores, sistemas de almacenamiento, conexiones, enrutadores, y otros sistemas virtualizados para manejar tipos generales de cargas de trabajo

2) **Plataforma como Servicio (PaaS)**: Servicios en los que se ofrece todo lo necesario para soportar el ciclo de vida completo de construcción y puesta en marcha de aplicaciones y servicios web disponibles en Internet. En este tipo de plataformas los desarrolladores pueden construir e implementar aplicaciones web en producción sin tener que instalar ninguna herramienta adicional.

3) **Software como Servicio (SaaS)**: Aplicación completa ofrecida como un servicio bajo demanda, vía multi-tenancy, que significa una sola instancia del software que se ejecuta en la infraestructura del Prestador de Servicios y sirve a múltiples clientes. Las aplicaciones que suministran este modelo de servicio son accesibles a través de un navegador web o de cualquier aplicación diseñada para tal efecto y el usuario no tiene control sobre ellas, aunque en algunos casos se le permite realizar algunas configuraciones.

Modelos de Implementación para *Cloud Computing*.

1) **Nube pública:** La infraestructura y los recursos lógicos que forman parte del entorno se encuentran disponibles para el público en general a través de Internet. Suele ser propiedad de un Prestador de Servicios que gestiona la infraestructura y el servicio o servicios que se ofrecen.
2) **Nube privada:** La infraestructura de la nube se aprovisiona para uso exclusivo de una única organización que comprende múltiples consumidores (por ejemplo, unidades de negocio). Puede ser propiedad, administrado y operado por la organización, un tercero o una combinación de ellos, y puede existir dentro o fuera de las instalaciones de la organización.
3) **Nube comunitaria:** La infraestructura en la nube se aprovisiona para uso exclusivo de una comunidad específica de consumidores de organizaciones que han compartido inquietudes (por ejemplo, misión, requisitos de seguridad, política y consideraciones de cumplimiento).
4) **Nube híbrida:** Término amplio que implica la utilización conjunta de varias infraestructuras en la nube de cualquiera de los tres tipos anteriores, que se mantienen como entidades separadas, pero que a su vez se encuentran unidas por la tecnología estandarizada o propietaria, proporcionando una portabilidad de datos y aplicaciones.

En este caso las ventajas e inconvenientes son los mismos que los relativos a los tipos de nube que incluya la infraestructura.

Tecnologías que no necesariamente son *Cloud.*

Se debe tener cuidado de considerar como *cloud* algo que finalmente no lo es, debido a que no cumpla con alguno de los requisitos fundamentales definidos en el capítulo anterior. En estos casos, los beneficios de su uso y las consideraciones en su implementación no pueden ser homologados con los descritos en esta guía, puesto que su naturaleza es diferente. Como muestra, presentamos algunos ejemplos de situaciones comunes donde algo *parece ser cloud, pero no lo es*:

1. Virtualización no necesariamente es *cloud*.
   Pese a que la virtualización de la infraestructura es un componente fundamental para habilitar la tecnología *cloud*, no todos los entornos de infraestructura y aplicaciones virtualizadas son entornos *cloud*. Para que puedan llamarse *cloud* deben cumplir con las cinco características señaladas en el párrafo anterior. Así, el tener un servidor virtualizado en un ambiente propietario y con aplicaciones para usuarios finales expuestos a internet, no será *cloud* si no tiene las características de elasticidad, autoservicio bajo demanda, recursos compartidos con otros sistemas, amplio acceso a la red y servicio medido.

2. Infraestructura tercerizada no necesariamente es *cloud*.
   Si cada vez que se requieren más o menos recursos de infraestructura para dar respuestas a las demandas ciudadanas es necesario realizar una serie de actividades administrativas y técnicas que permitan ampliar o disminuir los recursos, no estamos hablando de *cloud*. En cambio, si ante estos mismos requerimientos, se han establecido entre las partes umbrales de tolerancia que permitan en el mismo momento que están siendo requeridos aumentar o disminuir los recursos, ya sea en forma automática o con protocolos de autorización, se trata de un servicio *cloud* (por ejemplo, ante un alza en los accesos a una aplicación, si los recursos de las máquinas están en el 80% de su ocupación, se ha establecido entre las partes que los recursos de las máquinas se aumentarán en un 50%. Y esto se realiza en segundos, lo que permite mantener la disponibilidad contratada con buenos tiempos de acceso).

3. Acceso remoto a servicios o aplicaciones no necesariamente es cloud.
   Pese a que el modelo de servicio conocido como *Software as a Service* (definición en el próximo párrafo) es cada vez más utilizado, algunos Prestadores de Servicios lo interpretan solamente como acceso remoto a sus dependencias locales, sin contar con las características claves que definen a los servicios *cloud*, en particular, elasticidad, recursos compartidos y servicio medido, manteniendo los mismos paradigmas de los servicios instalados localmente, pero ahora bajo una óptica de acceso remoto.

Características y consideraciones al usar soluciones *cloud*

Características y Beneficios de las soluciones *cloud.*

En la medida en que las soluciones *cloud* se implementen adecuadamente y los flujos de trabajo sean los adecuados, pueden generarse grandes beneficios en torno al uso de esta tecnología, algunos de los cuales describiremos a continuación:

a. **Innovación,** la nube aporta entornos de procesamiento intensivo de datos de manera más ágil y flexible, y provee una plataforma común de colaboración entre entidades disímiles para el desarrollo de proyectos conjuntos, favoreciendo la armonización y estandarización de datos, sistemas y procesos.
b. **Economía,** toda vez que se elimina la inversión inicial en capital relacionado con infraestructura de servidores, almacenamiento, licencias, y se traduce a costos variables que se pagan cuando y cuanto sean necesarios, sin tener inversión ociosa, ahorrando en energía, mantenimiento y reparación del equipamiento, personal técnico para la operación, entre otros.
c. **Modernización de TI,** la nube permite disponibilizar en forma rápida y simple servicios digitales en múltiples dispositivos, agilizar las interacciones y la colaboración entre las instituciones públicas, maximizando así la capacidad de respuesta a las demandas ciudadanas.
d. **Disponibilidad,** generalmente los niveles de servicio ofrecidos por los Prestadores de Servicios Cloud son más exigentes que los ofrecidos en la informática tradicional, debido a que la nube permite migrar rápidamente ambientes que han presentado alguna falla y prevenir eventos que causen interrupciones de los servicios al facilitar la distribución geográfica y la redundancia de los recursos.
e. **Eficiencia,** producto de sus características intrínsecas, la nube permite a las instituciones lanzar sus aplicaciones en un menor tiempo, sin realizar inversiones de alto costo en equipamiento e implementación y configuración del mismo, incrementando la eficiencia de sus procesos, lo que habitualmente se traduce en menores costos y mayor rapidez en el desarrollo de las soluciones.
f. **Elasticidad, escalabilidad o pago por uso,** se contratan los servicios sólo cuando se requieren y la cantidad de ellos que se necesita. Las instituciones añaden o eliminan servicios evitando la compra de infraestructura y licencias. Por ejemplo, para el desarrollo de un sistema, si necesita un ambiente de pruebas, sólo mientras dure el proyecto se contratan los servidores virtuales con sus recursos y licencias, y se pagan sólo mientras los usa. O puede contratar un ambiente productivo que requiera más recursos (memoria, almacenamiento) durante un periodo acotado por la estacionalidad de su negocio. Lo mismo ocurre con la contratación de casillas de correo en la nube (o cualquier sistema en modalidad *SaaS* por usuario), si aumenta o disminuye el personal, el gasto se adecúa a ello.

g. **Ubicuidad,** sólo con tener conexión a internet los usuarios de las aplicaciones migradas a la nube pueden tener acceso desde cualquier lugar, y a través de cualquier dispositivo conectado, mientras así lo establezcan las reglas de acceso. Si se usa la Ofimática, los documentos o archivos podrán estar en ambientes compartidos y no en el equipo de un funcionario en su oficina, permitiendo el trabajo colaborativo sin estar físicamente en el mismo lugar.

h. **Fácil actualización,** habitualmente el software en modalidad *SaaS* se encuentra en su última versión y es actualizado automáticamente, por lo que el usuario lo tendrá disponible la siguiente vez que se conecte. Del mismo modo, los Prestadores de Servicios Cloud actualizan constantemente la infraestructura tecnológica que da soporte a sus servicios, por lo que es fácil utilizar siempre las últimas versiones de las plataformas tecnológicas, permitiendo así a los usuarios utilizar las actualizaciones de seguridad más recientes.

i. **Capacidad,** tecnológicamente hablando la nube tiene capacidad "ilimitada", ya que los Prestadores de Servicios Cloud pueden proveer la cantidad de almacenamiento y recursos de infraestructura que el cliente requiera en el tiempo, evitando así la compra de equipamiento especializado (storage, controladores, discos, licencias, otros), teniendo como límite el presupuesto vigente.

j. **Respeto al medio ambiente,** el uso de tecnologías *cloud* reduce la huella de carbono de una institución al ahorrar recursos que pasan de estar almacenados en equipos físicos a ser virtuales, por lo que pueden consolidarse entre distintos clientes o incluso en la misma institución, utilizando en promedio menor cantidad de infraestructura física y menor capacidad de procesamiento ocioso. Esto supone un considerable ahorro en consumo de energía, lo que es beneficioso para el medio ambiente.

k. **Disponibilización de ambientes de contingencia,** la nube es un medio ideal para disponer de infraestructura para algunos eventos de continuidad, puesto que se pueden conservar ambientes a menor escala que los ambientes de producción con el objetivo de minimizar las interrupciones, y sólo activarlos cuando sea necesario, sin incurrir en el costo periódico de mantenerlos todo el tiempo disponibles. Además, se puede aprovechar la diversa disponibilidad geográfica de los servicios para efectos de continuidad o distribución de respaldos.

Consideraciones y Cuidados al utilizar soluciones *cloud.*

Pese a la gran cantidad de ventajas que tiene la nube en flujos de trabajo equivalentes al ser comparado con los ambientes tradicionales, no podemos olvidar que también se deben tener algunas consideraciones específicas al considerar este tipo de servicios. Como un lineamiento general, se deberían abordar al menos los siguientes aspectos al considerar un servicio en la nube:

a. Manejo y Naturaleza de los Datos

Se recomienda revisar con detenimiento los contratos de prestación de servicios, y que éstos especifiquen claramente las mitigaciones a los riesgos identificados y las medidas de seguridad utilizadas para proteger los datos del Servicio. Es importante especificar estas medidas en un acuerdo de servicios o un contrato, para evitar situaciones en que sólo se

realizaron acuerdos o contratos no ejecutables o impracticables. También se debería prestar especial atención en la jurisdicción aplicable a los servicios contratados, considerando temas como la naturaleza de los datos tratados (en particular si se trata de datos personales), propiedad de los activos, leyes y regulaciones normativas aplicables, responsabilidades contractuales, interoperabilidad de los sistemas, utilizar formatos abiertos, etc.

Se deberían considerar aspectos relevantes al tratamiento de los datos, incluyendo registros y metadatos, a la gestión de salida, es decir, en el proceso de terminación de un contrato o acuerdo de prestación de servicios.

Para abordar los aspectos del manejo de datos, se sugieren los siguientes aspectos claves para determinar la naturaleza de los datos a utilizar en ambientes *cloud* y las medidas apropiadas que se deben tomar para protegerlos, incluyendo los posibles modelos de servicio e implementación de la nube que puedo o no utilizar:

i. Propiedad de los datos a tratar, incluyendo registros y metadatos. Es importante que la propiedad de un dato no sea modificada al ser tratada en entornos *cloud*.
ii. Localización geográfica y jurisdicción sobre los datos a tratar. Esto incluye cuando un Prestador de Servicios esté sometido a normas extranjeras que permitan la solicitud de información por parte de agencias estatales de otros países.
iii. Sensibilidad de los datos a tratar, incluyendo si se trata de datos personales, datos reservados o datos referentes a la seguridad nacional, que podrían tener exigencias específicas que deben ser analizadas caso a caso, pudiendo ser necesario descartar algunos modelos de servicio o implementación en la nube.
iv. Acceso y Eliminación de los datos tratados, definiendo claramente los períodos mínimos y máximos de retención de datos por parte del Prestador de Servicios.

b. Marco legal aplicable y condiciones contractuales

Se debería definir claramente el alcance de los servicios prestados y los márgenes de crecimiento o decrecimiento elástico del mismo. Esto es muy importante para no encontrar sorpresas durante la operación del servicio.
Se debería definir claramente los Acuerdos de Niveles de Servicios (SLA) y las sanciones en caso de incumplimiento. Los Niveles de Servicio acordados pueden incluir: tiempos de respuesta de la infraestructura, latencia, transaccionalidad soportada, tiempo de habilitación de infraestructura, tiempo en la gestión de los incidentes, u otros parámetros que se consideren relevantes.
Se debería definir claramente las políticas y procedimientos del prestador de servicios para la Gestión de Incidentes, incluyendo la notificación de los mismos a sus clientes, los procedimientos específicos para los incidentes de seguridad, Niveles de Servicio

comprometidos para la gestión de incidentes (ver punto anterior) y la gestión de un registro de incidentes puesto a disposición de las partes interesadas.
Se deberían considerar aspectos relevantes a la gestión de salida, en el proceso de terminación de un contrato o acuerdo de prestación de servicios, revisando temas como la duración máxima o mínima predefinida de los contratos, la posibilidad de finalizar el contrato cuando lo deseen, el plazo de aviso necesario para la terminación, la capacidad del Servicio de solicitar la rescisión del contrato y el tratamiento posterior de los datos, incluyendo registros y metadatos.

c. Evaluación estratégica de la Solución

En particular, para las soluciones *cloud* se requiere evaluar si estratégicamente constituyen una solución adecuada al problema que se desea resolver. Existen características claves que nos permiten identificar si un determinado proceso es apropiado para trasladarlo a entornos *cloud*. Algunos ejemplos de cargas de trabajo idóneas para implementar en la nube son:

- **Cargas de trabajo impredecibles o con potencial de crecimiento explosivo.** En particular, aplicaciones altamente populares o en constante crecimiento se benefician de disponer de capacidad elástica para no ser víctimas de su propio éxito. Por otra parte, se debe tener presente que sobre-aprovisionar infraestructura para casos extremos podría generar costos insostenibles a largo plazo.
- **Fluctuaciones de carga predecibles durante los períodos de alta demanda.** Si tenemos demanda con horas *peak* claramente definidas, podemos aumentar nuestra capacidad sólo para esas horas y así ahorrar recursos durante las horas de baja demanda. Lo mismo ocurre para procesos "*batch"*, los que se pueden disponibilizar sólo cuando sean necesarios, y el resto del tiempo mantener la infraestructura apagada o detenida.
- **Fácil paralelización del trabajo,** que permita un escalamiento horizontal más que vertical. Por ejemplo, procesamiento paralelo tales como *streaming*, codificación de video, solicitudes de contenido estático, entre otros, permiten utilizar múltiples instancias de procesamiento en lugar de una sola gran máquina.
- **Disponibilización de ambientes de contingencia.** En la nube podemos conservar ambientes a menor escala que los ambientes de producción, y sólo activarlos cuando sea necesario, sin incurrir en el costo periódico de mantenerlos todo el tiempo disponibles. Además podemos aprovechar la diversa disponibilidad geográfica de los servicios *cloud* para efectos de continuidad o distribución de respaldos.
- **Disponibilización de ambientes de Desarrollo y Pruebas.** La nube es un medio ideal para disponer de ambientes de desarrollo y pruebas, puesto que nos permite disponer de ambientes limpios, aislados y rápidamente disponibles para cada proyecto, y sólo activarlos cuando sea necesario, sin incurrir en el costo periódico de mantenerlos todo el tiempo disponible.
- **Ambientes no-críticos y ambientes de baja sensibilidad.** Los sistemas que no tratan datos reservados o que no sean parte de procesos críticos son los candidatos naturales para migrar a la nube en una primera instancia. Los

sistemas que están próximos a cumplir su ciclo de vida tecnológico también son candidatos a ser migrados, puesto que podrían evitar grandes inversiones en infraestructura y recursos tecnológicos al ser migrados directamente a la nube.

Del mismo modo, hay ciertas características de algunos procesos que hacen que las ventajas de llevarlos a *cloud* no sean tan claras, como, por ejemplo:

- **Aplicaciones que demanden muy baja latencia.** Un ejemplo de esta situación son las herramientas de captura y edición de audio, las plataformas financieras para compra y venta de acciones, protocolos para compartir archivos tales como NFS, SMB, etc, y otros.
- **Aplicaciones que requieran hardware especializado.** En caso de tener requerimientos específicos de hardware, ya sea por necesidades del negocio o por requerimientos regulatorios o normativos, se debería evaluar si éste es compatible con los ambientes en la nube. Un caso específico es la necesidad de dispositivos criptográficos para el almacenamiento de llaves o generación y cálculo de operaciones criptográficas, que sólo algunos Prestadores de Servicios disponen en modalidad *cloud*, y bajo condiciones específicas que lo hacen parecer más a un servicio de infraestructura tradicional que a uno *cloud*. Otro ejemplo es el hardware industrial específico o personalizado, que no tiene equivalentes en la nube.
- **Aplicaciones que utilicen protocolos inadecuados para la nube.** Habitualmente la problemática principal es la latencia, pero pueden existir otras razones por las que un protocolo no funciona en modalidad *cloud*. Hay ocasiones donde se pueden reemplazar algunos servicios de estas características por servicios que operen de forma adecuada en ambientes *cloud* (por ejemplo, un servidor NFS que operaría de forma deficiente en la nube puede ser reemplazado por recursos tipo S3 o Gluster, que permiten implementar una funcionalidad equivalente), pero esto debe ser analizado caso a caso por la organización.
- **Aplicaciones *legacy* que dependan de hardware no disponible en la nube.** Este es el caso de aplicaciones para mainframes, servidores AS400 u otros, que no tienen un equivalente *cloud*.

Por otra parte, pueden existir requerimientos específicos legales, normativos o regulatorios que impidan la migración de ciertas cargas de trabajo a algunos modelos de nube, como podría ser el caso ya mencionado de sistemas que traten datos altamente reservados o referentes a la seguridad nacional, para los que podría ser necesario el uso de modelos de nube privada o con requerimientos muy específicos que deban ser analizados caso a caso.

d. Seguridad en la Nube

Los usuarios de servicios *cloud* necesitan garantías de que los riesgos asociados al almacenamiento de sus datos y ejecución de sus aplicaciones en estos ambientes son comprendidos y gestionados adecuadamente. Al ser responsabilidad del Prestador de Servicios la implementación de algunas de las medidas de seguridad, se debería prestar particular atención a que los criterios de seguridad utilizados por el mismo sean

reconocidos, transparentes y verificables. Esto puede incluir auditorías o certificaciones externas que cumplan con estas características. Algunos principios de seguridad que los Prestadores de Servicios debieran cumplir son:

- **Controles de acceso, identidad y autenticación robustos:** El acceso a todas las interfaces de servicio debería restringirse a personas autenticadas y autorizadas para prevenir cambios no autorizados en el servicio del consumidor, robo o modificación de datos o la denegación de servicio.
- **Protección de los activos de información y datos, tanto en tránsito como en reposo:** Los centros de datos deberían estar construídos bajo estándares reconocidos de seguridad, para que los datos, activos y redes estén adecuadamente protegidos contra la manipulación, espionaje, pérdida, daño o incautación. Deberían existir criterios claros sobre el uso de controles criptográficos sobre los datos. Asimismo, debería existir una política clara de retención de datos, y plazos específicos para su posterior eliminación.
- **Seguridad Operacional, del Personal y Proveedores:** El Prestador de Servicios debería tener procesos y procedimientos establecidos para garantizar la seguridad en la operación del servicio, incluyendo la gestión de su personal y proveedores.
- **Gestión segura de los clientes, incluyendo separación de los mismos y promoción del uso seguro del servicio:** El Prestador de Servicios debería promover el uso seguro de sus servicios por parte de sus clientes, transmitiendo de forma clara las responsabilidades de cada parte cuando se use un servicio en la nube, para que este uso permanezca seguro y para que los datos de sus clientes estén adecuadamente protegidos. Parte de las responsabilidades del Prestador de Servicios en este ámbito es tomar las medidas adecuadas para garantizar la separación lógica o física de los clientes, según corresponda.
- **Proveer información de auditorías a los clientes:** Se debería poder proporcionar a los consumidores los registros de auditoría necesarios para controlar el acceso a su servicio y los datos contenidos en él, puesto que en algunos casos podría ser poco práctico o imposible para el cliente verificar personalmente el correcto cumplimiento de los contratos o acuerdos de servicio, lo que podría forzar a depender de certificaciones y auditorías de terceros. Este acceso debería ser razonable y respetando las políticas de confidencialidad.
- **Marco de gobernanza:** El Prestador de Servicios de servicios debería tener un marco de gobernanza de seguridad que entregue suficiente coordinación y dirija su enfoque en la gestión del servicio y la información que éste contiene.
- **Reporte de incidentes de seguridad:** El Prestador de Servicios debería transparentar al cliente información detallada y oportuna sobre los incidentes de seguridad que afecten el servicio contratado o a la información de éste y adoptar medidas para mitigar los posibles daños resultantes.

e. Disponibilidad de Auditorías y Estándares

En algunos casos podría ser poco práctico o imposible para el cliente verificar personalmente el correcto cumplimiento de los contratos o acuerdos de servicio, lo que podría forzar a depender de certificaciones y auditorías de terceros. El cliente debería determinar cuáles de estas certificaciones o auditorías son relevantes o útiles para sus intereses. Cabe destacar que el alcance de aplicación de algunas certificaciones o auditorías puede estar acotado sólo a ciertos procesos específicos, por lo que se recomienda solicitar todos los antecedentes que sean necesarios para garantizar que la confianza que estas certificaciones o auditorías nos dan en el Prestador de Servicios sea la adecuada. Se debería considerar también los casos en que el cliente necesite auditorías específicas, debiendo especificar claramente quién asume el costo de las mismas, quién selecciona al auditor y bajo qué condiciones se gatillan. En cualquier caso, el acceso a esta información debería ser provisto de forma razonable y respetando las leyes y políticas de confidencialidad vigentes.

f. Elasticidad

Se debería tener especial consideración el riesgo presupuestario que conlleva una planificación inadecuada de la capacidad. Especialmente en infraestructuras *cloud*, dada su naturaleza de servicio bajo demanda, no es difícil llegar a un punto en el que se pide más capacidad de lo presupuestado y, como consecuencia, el costo asociado también podría exceder el presupuesto original, por lo que deberemos tomar medidas adecuadas para que esto no ocurra, tales como hacer una buena planificación de la capacidad, reservar capacidad con anticipación o adoptar otras medidas que permitan definir en el contrato valores de crecimiento de manera flexible, que no obliguen necesariamente a realizar un nuevo proceso de compra.

Para establecer el costo estimado del proyecto a contratar se debería tomar en cuenta la demanda estimada del servicio, lo que nos obliga a identificar en detalle las distintas actividades asociadas y sus plazos, para poder determinar los recursos involucrados en cada una de ellas. Considere que los recursos necesarios en ambientes *cloud* pueden ser vastamente diferentes a los recursos tradicionales, en especial si comparamos modelos tradicionales con modelos *PaaS* o *SaaS*.

Un aspecto que debería ser considerado con particular atención son las posibles desviaciones del proyecto dentro de esta estimación referencial, incluyendo la demanda elástica y el posible crecimiento de los recursos utilizados, por lo que los costos podrían variar mes a mes. Para este propósito se recomienda realizar la estimación en base a las transacciones actuales de su servicio, las que se recomienda medir con anterioridad mediante herramientas especializadas para ello, métricas de servicios similares que se encuentren disponibles, transacciones estimadas futuras y tasas de crecimiento de las mismas, etc. Es muy importante también considerar la tecnología que se utilizará, puesto que hay tecnologías, lenguajes de programación, frameworks, etc, más livianos que otros, por lo que se debería también considerar este factor en la cubicación.

g. Monitoreo y Cumplimiento

Para una correcta operación de cualquier servicio tecnológico, es fundamental contar con visibilidad del mismo en forma de monitoreo de los servicios prestados. Se debería considerar que hay un sinnúmero de herramientas *nativas cloud* para el monitoreo en la nube, y que presentan importantes ventajas por sobre las herramientas de monitoreo

tradicional cuando las aplicamos en estos entornos, en particular, acceso a datos de la infraestructura *cloud* y no sólo de los servicios disponibles. Considerar que al estar ejecutándose en instancias virtualizadas y compartidas, las herramientas tradicionales, pensadas para un mundo de hardware local no siempre van a entregar una lectura completa o precisa del estado de nuestros sistemas, por lo que lo ideal es monitorear la infraestructura utilizando las herramientas apropiadas para ello, a menudo provistas por el mismo prestados de servicios *cloud* o por terceros especializados en la nube. Es habitual utilizar una combinación de herramientas de monitoreo para obtener mejores resultados. Se deberían establecer mecanismos para medir al menos los siguientes aspectos:

- cumplimiento de las medidas de seguridad acordadas
- cumplimiento de los niveles de servicio acordados.
- cumplimiento de las políticas del prestador de servicios.

Durante la operación del servicio por parte del proveedor, se debería considerar que se cumplan las políticas y procedimientos de gestión de incidentes establecidos durante la contratación, incluyendo la generación de registros de incidentes y su comunicación oportuna a las partes interesadas.

Referencias

NIST.2011. The NIST Definition of Cloud Computing. National Institute of Standards and Technology, U.S Departament of Commerce, Special Publication 800-145. De los autores Peter Mell y Timothy Grance, Septiembre 2011. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf [Consulta: 2 de enero 2018].