Aspectos Contractuales de Cloud Computing

Ana Sofía Zalazar[1], Silvio Gonnet[1], Horacio Leone[1]

[1] INGAR (UTN-CONICET) Avellaneda 3657, 3000 Santa Fe, Argentina
{azalazar, sgonnet, hleone}@santafe-conicet.gov.ar

Resumen. Cloud computing es un paradigma de negocio gestionado a través de protocolos de Internet. Cloud computing permite que los accesos a los servicios sean llevados a cabo por cualquier medio y dispositivo, de manera flexible y escalable. Los contratos y acuerdos de nivel de servicio cumplen un rol importante en las negociaciones entre el proveedor y consumidor de servicio, ya que en detallan los requerimientos funcionales y de calidad que un servicio debe cumplir. Sin normativas legales y contractuales que regulen las negociaciones en el contexto de cloud computing, los clientes potenciales deberán asegurarse que estos documentos abarquen aspectos funcionales, de calidad y aspectos de seguridad informática para todo el proceso de adquisición de servicios. En este trabajo se evalúan las características principales de cloud computing, se presentan recomendaciones en la contratación de servicios y se propone un modelo conceptual con los aspectos más relevantes de este paradigma.

Palabras Claves: Cloud Computing, Contrato, Acuerdo de Nivel de Servicio.

1 Introducción

Cloud computing, también conocido computación en la nube, es un paradigma de negocio gestionado a través de protocolos de Internet. Los proveedores de cloud computing ofrecen recursos informáticos y ejecución de tareas, utilizando técnicas de virtualización y economía en escala. Los clientes o consumidores de servicios sólo pagan lo que utilizan. Cloud computing permite que los accesos a los servicios sean llevados a cabo por cualquier medio y dispositivo, de manera flexible y escalable [1].

Para muchas organizaciones, este paradigma ha representado una manera de cubrir sus requerimientos de alta disponibilidad, fiabilidad y tolerancia a fallos, adquiriendo servicios de distribución geográfica muy dispersa. Del mismo modo, la aceptación de cloud computing depende ampliamente de la manera que los servicios cumplan con los requerimientos funcionales y no funcionales planteados por los consumidores [2][3]. Hanna et al. [4] analizan los requerimientos esenciales para contratar servicios en cloud computing y estos son: seguridad, privacidad, disponibilidad, auditoria, flexibilidad, almacenamiento, escalabilidad, y calidad de servicios. Repschlaeger et al. [5] presentan un marco de trabajo para la adopción de soluciones en cloud computing a través de un análisis de requerimientos y evaluación indicadores de servicios, dejando de lado el análisis de estos parámetros y los aspectos contractuales. En [6] se presenta un enfoque para la especificación de requerimientos en entornos de cloud

computing y una guía para la adquisición de servicios de software. Se podría considerar esta migración hacia cloud computing es un cambio de la estructura de sistemas empresariales, y es necesario analizar las cuestiones que implican la migración y la contratación de servicios en este paradigma. Cohen et al. [7] indica las cuestiones más relevante a considerar en la contratación y la migración de servicios. Luego Kaisler y Money [8] expande este trabajo de migración al contexto de cloud computing y considera que los desafíos actuales de este modelo son tres: adquisición: análisis de los proveedores, análisis de acuerdo de nivel de servicios, garantías de acceso a la información, y mejor costo/beneficio; implementación: adaptar datos a los formatos del servicio, desplegar servicios del cliente, escalar los recursos, y políticas de manejo de aplicaciones críticas; y seguridad y privacidad: movimiento de datos, control de acceso, eliminación de datos, auditorias, aspectos jurídicos y legales.

Debido al rápido crecimiento de cloud computing y desarrollo de la web profunda ("*deep web*") [9], algunas organizaciones internacionales están analizando la necesidad de una meta-legislación aplicable a Internet y de mayores normativas para protección de datos personales, propiedad intelectual, encriptación de contenidos sensibles, control de acceso a la información, monitoreo del tráfico de redes y seguridad informática. Por ejemplo, la European Network and Information Security Agency (ENISA) define y analiza los beneficios y riesgos de seguridad en cloud, desde una perspectiva técnica y legal [10]. Cloud Security Alliance (CSA) promueve el uso de las mejores prácticas en cloud para ofrecer garantías de seguridad [11]. El National Institute of Standard and Technology (NIST) creó un equipo para analizar los riesgos actuales que se presentan en la adopción de cloud computing [12].

Los contratos y acuerdos de nivel de servicio (SLA, Service Level Agreement) detallan los requerimientos funcionales y de calidad que un servicio debe cumplir. Debido a que son muchos los potenciales riegos y no existen normativas legales y contractuales que regulen las negociaciones en el contexto de cloud computing, los clientes potenciales deberán asegurarse que estos acuerdos abarquen cláusulas de disponibilidad del servicio, garantías del uso apropiado de información, mantenimiento de los recursos, y seguridad informática, tanto en la adquisición del servicio como en la terminación del contrato. Sí el proveedor no cumple con el nivel de servicio esperado, el consumidor deberá recibir una compensación acorde, que generalmente se refieren a una indemnización monetaria y créditos de servicio. Por lo tanto, el monitoreo continuo de los niveles de servicios es uno de los aspectos más importantes para asegurar que se cumplen los acuerdos establecidos.

En este trabajo se presentan los aspectos contractuales más importantes de cloud computing, algunas recomendaciones para la adquisición de servicios y un modelo conceptual para formalizar las bases de un contrato de servicio y el desarrollo de SLA, considerando las vistas propuestas por Zalazar et al. [13]. A continuación se realiza una síntesis de las características principales de cloud computing, sus modelos de despliegues y sus modelos de servicio. Luego, en la Sección 3 se analizan los tipos de contratos para cloud computing (unilateral y negociables) y se presentan algunas recomendaciones para la creación de contratos legales. La Sección 4 presenta el modelo conceptual para la adopción de servicios en un marco de negocio, que servirá para reunir criterios de evaluación y aspectos importantes para la creación de contratos. Finalmente, la Sección 5 discute las conclusiones finales.

2 Características de Cloud Computing

Debido a la diversidad de información y enfoques que tiene el paradigma de cloud computing, no existe una definición unificada [14][15]. El NIST propone una definición que abarca los aspectos más generales de este modelo de negocio [16]: "*Cloud computing es un modelo que permite acceso a redes bajo demanda, para compartir un conjunto de recursos de computación configurable (es decir, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente provistos o liberados con un mínimo esfuerzo de administración o interacción con los proveedores de servicio*" [1]. Bajo el marco de esta definición, se puntualizan cinco características principales (*On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, y Measured Service*), cuatro modelos de despliegue de servicio (*Private Cloud, Community Cloud, Public Cloud, y Hibrid Cloud*) y tres modelos de servicio (*Software as a Service - SaaS, Plataform as a Service - PaaS y Infraestructure as a Service - IaaS*). Además, NIST define cinco roles: *Consumidor:* entidad que utiliza el servicio; *Proveedor:* entidad responsable de la disponibilidad del servicio; *Transportador:* intermediario que ofrece conectividad y exportación de datos para utilizar los servicios provistos; *Bróker:* intermediario que se involucra en la relaciones contractuales y de negocio; y *Auditor:* agente externo que se encarga de informar el estado de los servicios.

Los entornos de cloud computing consiste en un conjunto de recursos físicos que son optimizados para maximizar su rentabilidad, incrementando los servicios ofrecidos y minimizando los costos totales. Los proveedores pueden reemplazar los dispositivos con fallas crecientes, desconectar unidades de hardware que no son utilizadas cuando la demanda de servicios es baja, o bien conectar nuevas unidades para atender las nuevas demandas [12]. Es el modelo de despliegue quien define si estos recursos son de acceso exclusivo de determinada organización o compartidos, si se encuentran en el centro de datos del cliente ("*on-premises"*) o en el servidor de los servicios ("*off-premises"*). En consecuencia, se debe analizar en los contratos y acuerdos de servicios el modelo de despliegue ofrecido por el proveedor, ya que indica los riegos asumidos durante el contrato de negocio, además los parámetros de seguridad que deberán ser configurados para el acceso de los diferentes consumidores de servicios. Los distintos modelos de despliegues son:

- *Nube Privada*. Los recursos y accesos son de uso exclusivo de una organización.
- *Nube Comunitaria*. Los recursos son compartidos por una comunidad de organizaciones específicas, que poseen alguna característica especial que la hacen formar parte de esta comunidad. Estas comunidades obligan al proveedor a compartir políticas específicas entre los usuarios de la nube comunitaria.
- *Nube Pública*. Los servicios se encuentran alocados dentro de los servidores del proveedor o de terceras partes. La infraestructura de la nube es compartida por varios clientes independientes y se debe asegura la independencia entre los entornos de estos clientes.
- *Nube Híbrida.* Es una combinación de una nube privada, nube pública o nube comunitaria.

Los servicios prestados por los proveedores de cloud computing se pueden clasificar en tres modelos o tipos de servicio, considerando el "Modelo SPI" (Software, Plataforma e Infraestructura) [17]. Según el modelo adoptado son las características de abstracción brindadas de los recursos físicos y los permisos necesarios que el proveedor debe otorgar al consumidor de servicio. En consecuencia, el consumidor deberá reforzar la seguridad informática y preservación de los datos según el modelo elegido, utilizando mecanismos dentro de su perímetro de control. Los modelos disponibles dentro del enfoque SPI son:

- *Software como un Servicio (SaaS).* El servicio está formado por aplicaciones que los usuarios finales pueden acceder a través de uso de navegadores o interfaces web en los dispositivos utilizando protocolos de Internet, y el proveedor enmascara el hardware que soporta la capa lógica de las aplicaciones.
- *Plataforma como un Servicio (PaaS).* El servicio ofrecido es un contenedor que posee un entorno de programación, con bibliotecas y herramientas que dan soporte al desarrollo de aplicaciones.
- *Infraestructura como un Servicio (IaaS).* El servicio está dado por máquinas virtuales, capacidad de almacenamiento, base de datos y dispositivos de redes.

3 Tipos de Contratos y Recomendaciones de Análisis

La información, los datos y las aplicaciones propietarias de un consumidor de cloud computing deben considerarse como bienes activos, ya que poseen un valor económico intangibles, por lo que se hace necesaria la instalación de controles destinados a su protección. Para adquirir servicios en cloud computing, las organizaciones deben depositar estos activos en los recursos físicos de los proveedores de servicio. Por lo tanto, los acuerdos de servicios y contratos deben estar cuidadosamente escritos, contemplando todos los detalles posibles de transferencia, almacenamiento, recuperación y acciones al término del contrato. Además se debe contemplar, las acciones a tomar si ocurre algún evento como el robo, pérdida y corrupción de la información, como también los mecanismos de encriptación y protección de la propiedad intelectual. Se debe tener en cuenta que donde estén alocados los datos es donde se deberá respetar la legislación y por lo tanto consultar los marcos regulatorios de la jurisdicción donde se realice el almacenamiento y procesamiento de datos.

Las características básicas de seguridad que deben estar contempladas en un contrato de servicio son: a) autenticidad: es la garantía de que el origen y el destino de la información son de usuarios o procesos debidamente autorizados; b) integridad: aseguramiento de que el contenido de los datos y servicios permanecen invariable a menos que sea modificado por un usuario o un proceso debidamente autorizado, es decir que la información fue adulterada o destruida; c) operatividad: los servicios y la datos son accesibles durante el tiempo estipulado que dura el contrato; y d) confidencialidad: la garantía que la información es conocida por los usuarios y procesos debidamente autorizados [18].

Existen dos tipos de modelos de contratos para la adhesión y adquisición de servicios de cloud computing: modelo unilateral y modelo negociable [19].

3.1 Contrato Unilateral de Adhesión a Servicios

Este modelo de contrato es muy común en aquellos usuarios de Internet, que utilizan servicios estándares y servicios de proveedores gratuitos (cuentas de e-mails, redes sociales, álbum fotográfico, repositorio de almacenamiento, etc.). Generalmente la suscripción a estos servicios gratuitos, permite que el consumidor del servicio pueda acceder a sus datos y a los servicios provistos desde cualquier dispositivo, utilizando mecanismos sencillos de autenticación y protocolos de acceso a Internet.

Los proveedores de estos tipos de servicios ofrecen contratos estáticos y predefinidos para todos los consumidores de servicio. Como contrapartida, estos tipos de contratos protegen los intereses propios de la parte proveedora y pueden restringir severamente el monitoreo en los mecanismo de entrega del servicio. Al mismo tiempo, estos acuerdos pueden ser incompletos y presentar términos ambiguos que hacen difícil la evaluación de los riesgos asociados al optar por un determinado proveedor. Por ejemplo, en los términos de contrato el proveedor puede indicar que escaneará los datos del consumidor almacenados en sus servidores y utilizará la información adquirida para ofrecer publicidades a medida.

Además, en estos tipos de contratos, el proveedor puede restringe su responsabilidad ante las fallas ocasionadas durante los cortes programados de servicios, los eventos de fuerza mayor fuera de su alcance, y las violaciones de seguridad. También reservan el derecho de cambiar el acuerdo de servicio, y modificar los servicios, sin previo aviso y publicando las modificaciones directamente en su página web. Sin embargo, se exige a los consumidores respetar los términos de servicio, abstenerse de almacenar contenidos ilegales en los entornos del proveedor y comprometerse a no realizar ningún tipo de acciones fraudulentas, cumpliendo con la jurisdicción donde se encuentran los dispositivos físicos del proveedor.

La mayoría de estos servicios se encuentran en nube públicas y las conexiones a las interfaces del servicio se realiza mediante la utilización de navegadores. El nombre del dominio o URL ("*Uniform Resource Locator*"), que se coloca en el navegador, es traducido mediante los servidores DNS ("*Domain Name System*") a etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz ("*API*") de un dispositivo dentro de una red que utilice el protocolo IP ("*Internet Protocol*").

Sin embargo, es probable que un atacante o usuario malicioso se valga de la dirección IP de los recursos de determinado servicio de cloud computing, para acceder a los datos del consumidor. En los últimos años se han registrado estos tipos de accesos fraudulentos a las cuentas de usuario, robos de identidad, y violaciones de la privacidad, acciones maliciosas que aprovecharon la brecha de seguridad en los servidores de servicios. Algunos ataques pueden hasta generar un gran número de "*botnet*", que son algoritmos que enciende un gran número de máquinas "*zombie*" para enviar paquetes a la web del servidor generando congestión en la comunicación [20].

Por lo tanto, el navegador y la red de acceso del consumidor de servicio deben estar libre de vulnerabilidades en la seguridad, tráfico malicioso y atacantes. Aunque los servicios sean estándares o gratuitos, es recomendable adoptar siempre el mayor nivel posible de seguridad, y realizar un estudio minucioso de riesgos e impactos. Por ejemplo, se podría acceder a la interfaz del proveedor utilizando algún protocolo de cifrado en los navegadores ("*Security Socker Layer*"), registrar los accesos y monitorear el tráfico de la red.

3.2 Contrato Negociable de Adquisición de Servicios

Los contratos negociables o personalizados de adquisición de servicio son adecuados para clientes de cloud computing que necesitan algún trato especial en sus operaciones o trabajan con datos sensible. Estos consumidores potenciales de servicios deben consultar con brókeres, consultores tecnológicos y agentes especializados en contratos. Probablemente, exista la necesidad de implementar cloud privadas para localizar las aplicaciones propietarias del consumidor del servicio y proteger los datos confidenciales, mientras se beneficia de las bondades que ofrece cloud computing como paradigma de negocio. El consumidor de servicio se debe asegurar que existen cláusulas de confidencialidad y políticas de seguridad en estos contratos.

Debido a la especialización de los términos de servicios que se requieren para este tipo de contrato, uno de los riesgos asociados es "*provider lock in*", técnica que utilizan la mayoría de los proveedores de servicios para que un consumidor se mantenga dependiente de los servicios que estos proveen. Por lo tanto, se recomienda indicar explícitamente los mecanismos adicionales de transferencia de datos, migración de entornos y despliegue de servicios hacia otros proveedores, en el periodo de extinción del contrato. Del mismo modo, el consumidor de servicio debe estar atento de los cambios que realice el proveedor en sus entornos, ya que podría traer asociado complejidad para cambiar de proveedor.

En esto tipos de contratos se debe identificar todos los aspectos contractuales (funcionales, calidad, jurídicos y legales), al mayor detalle posible. Estos contratos deben evitar interpretaciones ambiguas y limitar las responsabilidades de las partes. También deben incluir cláusulas de acceso de datos, seguridad de información, monitoreo y control de los servicios, medidas de resguardo de datos y recuperación del servicio. Todas las políticas y procedimientos que se llevarán a cabo para el transporte, almacenamiento y procesamiento de datos, durante el contrato y el periodo de extinción del mismo (destrucción de la información del cliente en los entornos del proveedor).

En [21] se indican una lista de partes del contratos donde el consumidor de servicio debe centrar especial atención al momento de la negociación. Las más relevantes son: nivel de servicio; confidencialidad; disponibilidad; rendimiento; seguridad; plan de continuidad y recuperación ante desastres; facturación de servicios suspensión del servicio; servicios de soporte; terminación o modificación del contrato; privacidad y cumplimiento normativo; notificaciones de brechas de seguridad y procesos legales; uso de datos del cliente; y compensación e indemnización.

3.3 Recomendaciones Legales para Contrataciones

En el documento publicado por ENISA [10] se presentan las recomendaciones legales para los clientes reales y potenciales de los servicios de cloud computing. A continuación se resumen estas recomendaciones, que deben ser analizadas en todas las contrataciones de servicios en cloud computing:

- *Protección de datos.* Control de medidas técnicas de seguridad adecuada y medidas organizativas de protección de datos. El cliente debería analizar cuidadosamente este apartado en el contrato, para determinar si el proveedor ofrece las suficientes

garantías de tratamiento lícito y las compensaciones acordes a los daños potenciales de la violación de estas cláusulas.

- *Seguridad de los Datos.* Respetar las medidas obligatorias a escala nacional y supranacional de seguridad de los datos. En el terreno legal, un lugar físico se refiere a una jurisdicción y las autoridades pueden confiscar los datos si no se cumplen las leyes locales. El proveedor debe estar obligado a notificar a sus clientes cuando existen amenazas o incidentes de seguridad que involucren sus datos, principalmente que afecten la integridad, la confidencialidad y la disponibilidad de la información del cliente.
- *Transferencia de información.* Se debe prestar atención a la transferencia e intercambio de información, dentro y fuera de la jurisdicción de los consumidores y los proveedores. Garantizar la protección adecuada de los datos, aun cuando el origen/destino de la transferencia sea de diferente jurisdicción.
- *Acceso a las autoridades policiales.* Analizar las restricciones y requisitos necesarios de las autoridades policiales sobre la jurisdicción en la que los datos pueden almacenarse, procesarse y evaluar cualquier riesgo derivado a esto.
- *Confidencialidad y no divulgación.* Funciones y obligaciones referidas a esta cuestión. El cliente potencial debería analizar las políticas de confidencialidad y no divulgación de sus datos y saber qué información del cliente circulará en los entornos de cloud computing.
- *Propiedad intelectual.* Explicitar que se respeta los derechos del cliente de cloud computing, sobre cualquier propiedad intelectual o trabajo original. Esta cláusula deberá ser lo suficientemente detallada y las infracciones deben ser sustanciales, para que el proveedor garantice la protección de la información del cliente.
- *Asignación de riesgos y limitación de la responsabilidad.* Considerar las obligaciones que plantean los riesgos y los límites de responsabilidad, incluyendo cláusulas de compensación económica y obligaciones de indemnización por la parte que no cumpla con los contratos. Los errores en los servicios pueden tener impacto en la capacidad del cliente y sus obligaciones para con sus propios clientes, por lo que debe analizarse las responsabilidades contractuales por negligencia. También debe evaluarse las condiciones del contrato que atribuyen responsabilidad al cliente por cualquier actividad ilegal realizada utilizando las cuentas autenticadas por el cliente, sin que este las realice.
- *Servicios de subcontratación y cambio de control.* Capacidad para continuar las obligaciones contractuales en caso de producirse un cambio de control, o bien la posibilidad de rescindir el contrato. El cliente puede exigir que los cambios de control o subcontratación estén sujetas a su autorización previa.

4 Modelo Conceptual para brindar soporte a la Contratación de Servicios.

El modelo propuesto en la Fig. 1 tiene la finalidad de servir como base para la captura de datos relevantes sobre contratos y acuerdos de nivel de servicio dentro del contexto

de cloud computing. Esta propuesta extiende los conceptos introducidos en la contribución [13], añadiendo a los aspectos contractuales el término de *jurisdicción*.

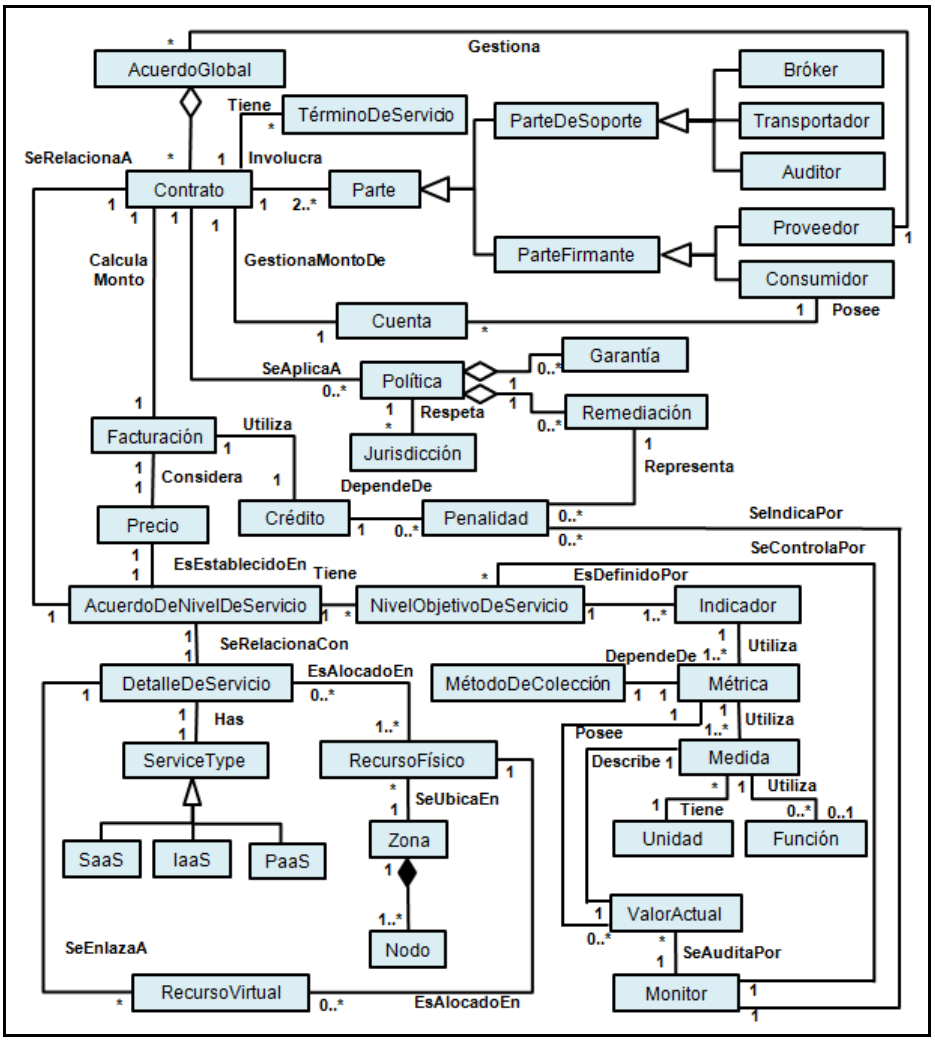

Fig. 1. Vista de Control

En los contratos de servicio, tal como se detalla en la sección 4, se deben tener en cuenta la jurisdicción del lugar donde se encuentran alocados los datos del cliente y los servicios del proveedor, ya que representará la legislación y los marcos regulatorios que los contratos de servicios deberán respetar para evitar problemas legales.

El modelo permite tanto la representación de contratos unilaterales como negociables, y además considera las distintas recomendaciones realizadas por el ENISA y el NIST, detalladas en las secciones previas. Por ejemplo: es posible representar las

políticas asociadas a los contratos las cuales deben ser respetadas durante el plazo de duración del mismo y la etapa de extinción, por lo general son cláusulas personalizadas según los requerimientos del consumidor. Esta políticas pueden representar una o varias jurisdicción, y además pueden ser del tipo de *garantía* (seguridad, integridad, confidencialidad, etc.) o políticas de *remediación* que se llevan a cabo cuando algún aspecto del contrato no ha sido respetado o los *niveles objetivos del servicio* no han sido alcanzados. Esta remediación indica una *penalización*, que generalmente calcula *créditos* a favor del consumidor.

El *nivel objetivo de servicio* es definido por uno o más *indicadores*. Los *indicadores* pueden ser de rendimiento, velocidad de procesamiento, ancho de banda, latencia en los sistemas, entre otros. Los *indicadores* utilizan *métricas*, que se asocia a una determina *medida*, y esta tiene una *unidad* y una *función* de cálculo.

Los *valores actuales* de la *métricas* se van generando de acuerdo al *métodos de colección* (por nanosegundo, minuto, horas, etc.) que estas posean.

El *monitor* de servicio deberá auditar los valores e indicar cuándo se encuentren fuera del *nivel objetivo de servicio*, que es donde se indicará una *penalidad* a ejecutar.

6 Conclusiones

En el presente trabajo se tienen en cuenta las diferentes recomendaciones de los distinto actores participantes de cloud computing, para formular un modelo conceptual que brinde el soporte adecuado en la contratación de servicios, y permita el monitoreo del cumplimiento de las cláusulas del contrato.

Por lo tanto, el modelo propuesto permite asociar los aspectos contractuales a métricas mesurables. En caso de que algún evento ponga en manifiesto el no cumplimiento de estos contratos y violación de políticas de seguridad, se podrán contar estas métricas y registros acceso para este análisis.

El modelo conceptual es genérico y puede aplicarse a todos los modelos de despliegue y los modelos de servicio, también a los contratos unilaterales y los contratos negociables.

La migración de servicios a cloud computing puede considerarse un cambio en la estructura de los contratos de negocios, y los procedimientos jurídicos. Es por esto, que se necesita de herramientas, como este modelo, que identifiquen la relación de la tecnología con la legislación.

Además, el análisis realizado en este trabajo permite identificar los potenciales riesgos en el contexto de cloud computing, que hacen referencia a la seguridad de la información, la implementación de políticas y los controles para la gestión de los servicios.

Agradecimientos. Este trabajo ha sido financiado en forma conjunta por CONICET, la Universidad Tecnológica Nacional y la Agencia Nacional de Promoción Científica y Tecnológica. Se agradece el apoyo brindado por estas instituciones.

Referencias

1. Mell, P., Grance, T.: The NIST definition of cloud computing. NIST special publication 800-145 (2011)
2. Khaddaj, S.: Cloud Computing: Service Provisioning and User Requirements. In Distributed Computing and Applications to Business, Engineering & Science (DCABES), 2012 11th International Symposium on. IEEE (2012) 191-195
3.Schmidt, R.: Augmenting Cloud Requirements Engineering with Meta-Services. In Computer Software and Applications Conference Workshops (COMPSACW) 2011 IEEE 35th Annual. IEEE (2011) 488-493
4. Hanna, E. M., Mohamed, N., Al-Jaroodi, J.: The Cloud: Requirements for a Better Service. In Cluster, Cloud and Grid Computing (CCGrid), 2012 12th IEEE/ACM International Symposium on. IEEE (2012) 787-792
5. Repschlaeger, J., Zarnekow, R., Wind, S., Klaus, T.: Cloud Requirement Framework: Requirements and Evaluation Criteria to adopt Cloud Solutions (2012)
6. Zalazar, A. S., Gonnet, S., Leone, H.: Especificación de Requerimientos para Sistemas que emplean Servicios Web en Cloud Computing. 1er Congreso Nacional de Ingeniería Informática / Sistemas de Información (CoNaIISI 2013), en prensa. Argentina (2013)
7. Cohen S., Money W. H., Kaisler S. H.: Service Migration in an Enterprise Architecture. Proceeding of the 42nd Hawaii International Conference on System Sciences. Hawaii (2009)
8. Kaisler, S. H, Money, W. H.: Service Migration in a Cloud Computing. Proceeding of the 44th Hawaii International Conference on System Sciences. Hawaii (2011)
9. Shestakov, D.: Deep Web: databases on the Web. Entry in Handbook of Research on Innovations in Database Technologies and Applications: Current and Future Trends (2009)
10.Catteddu, D.: Cloud Computing: benefits, risks and recommendations for information security. Springer Berlin Heidelberg (2010)
11.Brunette, G., Mogull, R.: Security guidance for critical areas of focus in cloud computing v2. 1. Cloud Security Alliance (2009) 1-76
12.Badger, L., Grance, T., Patt-Corner, R., Voas, J.:Cloud computing synopsis and recommendations. NIST special publication. 800-146 (2012)
13.Zalazar, A. S., Gonnet, S., Leone, H.: Un Modelo para Contratos de Cloud Computing. 42JAIIO – 14 Simposio Argentino de Ingeniería de Software (ASSE 2013) Argentina (2013) 303-317
14.Foster, I., Zhao, Y., Raicu, I., Lu, S.: Cloud computing and grid computing 360-degree compared. In Grid Computing Environments Workshop. GCE'08. IEEE (2008) 1-10
15.Vaquero, L. M., Rodero-Merino, L., Caceres, J., Lindner, M.: A break in the clouds: towards a cloud definition. ACM SIGCOMM Computer Communication Review. (2008) 50-55
16.Bass, L., Clements, P., Kazman, R.: Software architecture in practice. Addison-Wesley Professional (2003)
17.Winkler, V. J.: Securing the Cloud: Cloud computer Security techniques and tactics. Elsevier (2011)
18.Cherdantseva, Y., Hilton, J.:A Reference Model of Information Assurance & Security. In Availability, Reliability and Security (ARES) 2013 Eighth International Conference on (pp. 546-555). IEEE (2013)
19.García del Poyo, R.: Cloud Computing: Aspectos jurídicos claves para la Contratación de estos Servicios. Revista Española de Relaciones Internacionales (2012) 48-91.
20.Sabahi, F.: Cloud computing security threats and responses. In Communication Software and Networks (ICCSN) 2011 IEEE 3rd International Conference on. IEEE (2011) 245-249
21.Pérez San-José, P., Gutiérrez Borge, C., Álvarez Alonso, E., De la Fuente Rodríguez, S., García Pérez, L.: Guía para empresas: seguridad y privacidad del cloud computing. Instituto Nacional de Tecnologías de la Comunicación, INTECO (2011)