Naciones Unidas A/CN.9/WG.IV/WP.148

Asamblea General

Distr. limitada
30 de enero de 2018
Español
Original: inglés

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
Grupo de Trabajo IV (Comercio Electrónico)
56º período de sesiones
Nueva York, 16 a 20 de abril de 2018

Aspectos contractuales de la computación en la nube

Nota de la Secretaría

Índice

V.18-00392 (S) 060318 060318

I. Introducción

1. El Grupo de Trabajo tal vez desee remitirse a los párrafos 1 a 6 del documento A/CN.9/WG.IV/WP.142 para obtener información de antecedentes sobre el trabajo realizado en materia de computación en la nube antes del 55º período de sesiones del Grupo de Trabajo (Nueva York, 24 a 28 de abril de 2017). En el programa provisional del período de sesiones en curso se ofrece un resumen de los avances realizados por el Grupo de Trabajo en su 55º período de sesiones y por la Comisión en su 50º período de sesiones (véase el documento A/CN.9/WG.IV/WP.147, párrs. 7 y 8).

2. De conformidad con la recomendación del Grupo de Trabajo sobre la posible labor futura en materia de computación en la nube (A/CN.9/902, párr. 23) y las opiniones expresadas al respecto en el 50º período de sesiones de la Comisión[1], la Secretaría presenta al Grupo de Trabajo para su examen un proyecto de lista de verificación que incluye las principales cuestiones relacionadas con los contratos de computación en la nube. El proyecto de lista de verificación, elaborado por la Secretaría con la participación de expertos, refleja las consideraciones preliminares formuladas por el Grupo de Trabajo en lo que respecta al ámbito de aplicación y al contenido que podría tener una lista de verificación, así como a los criterios para su redacción (A/CN.9/902, párrs. 11 a 28).

3. Se prevé que el Grupo de Trabajo informe sobre los progresos de su labor en materia de computación en la nube a la Comisión en su 51º período de sesiones (Nueva York, 25 de junio a 13 de julio de 2018)[2]. Teniendo en cuenta quiénes serán los probables destinatarios de la lista de verificación y las transacciones para las cuales se prevé que se utilice, el Grupo de Trabajo tal vez desee considerar si la lista debería elaborarse como un instrumento de referencia en línea. En ese caso, el Grupo de Trabajo tal vez desee recomendar a la Comisión dicha posibilidad y, en concreto, sugerir que la Secretaría elabore un instrumento de referencia en línea que refleje el contenido sustantivo del proyecto de lista de verificación en su versión revisada por el Grupo de Trabajo en su 56º período de sesiones y por la Comisión en su 51º período de sesiones.

II. Proyecto de lista de verificación sobre las principales cuestiones que podrían plantear los contratos de computación en la nube

[*Los términos que aparecen en negrita en la lista de verificación se describen en el glosario que figura a continuación de la lista. En un instrumento de referencia en línea podrían explicarse de una forma más sencilla para el usuario*.]

Introducción

1. En la lista de verificación se abordan las principales cuestiones que podrían plantear los contratos de computación en la nube firmados por entidades mercantiles en los que una de las partes (el proveedor) proporciona a la otra (el cliente) uno o más **servicios de computación en la nube** para un usuario final. Los contratos de reventa u otras formas de distribución de los **servicios de computación en la nube** están excluidos del ámbito de aplicación de la lista de verificación. Asimismo, quedan excluidos de su ámbito de aplicación los contratos de **servicios de computación en la nube firmados con colaboradores** y otros terceros que puedan participar en la prestación de estos servicios al cliente (por ejemplo, los contratos firmados con subcontratistas o proveedores de servicios de Internet).

[1] *Documentos Oficiales de la Asamblea General, septuagésimo segundo período de sesiones, Suplemento núm. 17* (A/72/17), párrs. 116 a 127.

[2] *Ibid.*, párrs. 116 y 127.

2. Los contratos de computación en la nube pueden llegar a calificarse en función de lo previsto en la legislación aplicable como un contrato de servicios, de alquiler, de externalización, de licencia, como un contrato mixto o de otro tipo. Los requisitos legalmente previstos en cuanto a su forma y contenido pueden, por tanto, variar. En algunas jurisdicciones, las propias partes en el contrato pueden calificarlo como de un tipo determinado cuando la legislación es ambigua o no se pronuncia sobre esa cuestión. Los tribunales pueden tener en cuenta esta calificación a la hora de interpretar las cláusulas del contrato, a menos que ello sea contrario a la ley, a la práctica de los tribunales, a la verdadera intención de las partes, a las circunstancias del caso o a las costumbres o prácticas comerciales.

3. Las cuestiones abordadas en la presente lista pueden aparecer en los contratos de computación en la nube, con independencia del tipo de **servicios de computación en la nube** de que se trate (por ejemplo, **IaaS**, **PaaS** o **SaaS**), de su **modelo de despliegue** (por ejemplo, **público, compartido, privado** o **híbrido**) y de las condiciones de pago (con o sin remuneración). La lista de verificación se centra en los contratos de **servicios de computación en la nube** de tipo **SaaS público** con remuneración.

4. La capacidad para negociar las cláusulas de los contratos de computación en la nube dependerá de muchos factores, en especial de si el contrato versa sobre **soluciones de nube genéricas y estandarizadas para múltiples suscriptores** o sobre una solución personal, hecha a medida; de si existen o no ofertas competidoras, así como de las posiciones de negociación de las partes en el contrato. La capacidad para negociar las condiciones de un contrato (en especial las cláusulas sobre suspensión, resolución o modificación unilateral del contrato por parte del proveedor y las cláusulas de responsabilidad) puede ser un factor importante a la hora de elegir un proveedor en los casos en los que es posible elegir [*cross-link*]. Aunque la lista de verificación ha sido elaborada, principalmente, para las partes que negocian un contrato de computación en la nube, también puede resultar útil para los clientes que deseen revisar las condiciones estándar ofrecidas por los proveedores con el fin de determinar si dichas condiciones se ajustan a sus necesidades.

5. Las partes no deben considerar esta lista de verificación como una fuente de información exhaustiva sobre la redacción de contratos de computación en la nube ni como un sustituto del asesoramiento jurídico y técnico o de los servicios de asesores profesionales competentes. En la lista se señalan algunas cuestiones que las quienes consideren la posibilidad de suscribir un contrato deberían tener en cuenta antes y durante su redacción, sin pretender transmitir la idea de que todas estas cuestiones deban considerarse siempre. Las diversas soluciones propuestas a las cuestiones examinadas en la lista de verificación no se aplicarán a las relaciones entre las partes a menos que estas las acepten expresamente, o a menos que las soluciones resulten de lo dispuesto en la ley aplicable. Ni los títulos ni los epígrafes utilizados en la lista de verificación ni su orden deben considerarse obligatorios ni debe entenderse que se sugiere una determinada estructura o estilo para los contratos de computación en la nube. La forma, el contenido, el estilo y la estructura de los contratos de computación en la nube pueden variar considerablemente según las diversas tradiciones jurídicas, estilos de redacción, requisitos legales, y necesidades y preferencias de las partes.

6. [La lista de verificación no debe entenderse como una expresión de la opinión de la CNUDMI sobre la conveniencia de celebrar contratos de computación en la nube.]

7. La lista de verificación consta de dos partes y un glosario: en la primera parte se abordan los principales aspectos precontractuales que las futuras partes, primordialmente el cliente, podrían tener en cuenta antes de firmar un contrato de computación en la nube; en la segunda, se abordan las principales cuestiones contractuales que las partes podrían necesitar resolver al redactar un contrato de computación en la nube; y en el glosario se describen algunos de los términos técnicos utilizados en la lista a fin de facilitar su comprensión.

Primera parte. Principales aspectos precontractuales

A. Verificación de la existencia de normas imperativas y otros requisitos

8. El marco jurídico aplicable al cliente, al proveedor o a ambos puede imponer ciertas condiciones para la celebración de un contrato de computación en la nube. Estas condiciones pueden también tener su origen en obligaciones contractuales, como las que surgen de las **licencias de propiedad intelectual**. El cliente y el proveedor deben prestar especial atención a las leyes y los reglamentos sobre **datos personales**, ciberseguridad, control de las exportaciones, aduanas, impuestos, secretos comerciales, propiedad intelectual y a la **normativa específica de cada sector** a la que, tanto ellos como sus futuros contratos, puedan estar sujetos. El incumplimiento de los requisitos obligatorios puede acarrear importantes consecuencias negativas como la invalidez o la inexigibilidad del contrato, o de una parte del mismo, multas administrativas y responsabilidad penal.

9. Las condiciones para celebrar un contrato de computación en la nube pueden variar por sector y jurisdicción. Pueden incluir la obligación de adoptar medidas especiales para proteger los **derechos de los sujetos de los datos**, desplegar un determinado modelo de servicio (nube **privada**, en lugar de **pública**), cifrar los datos alojados en la nube y registrar ante las autoridades del Estado una transacción o un programa informático utilizado en el tratamiento de los **datos personales**. También pueden incluir requisitos de **ubicación de los datos**, así como requisitos relativos al proveedor.

- *Ubicación de los datos*

10. Los requisitos de **ubicación de los datos** pueden derivarse especialmente de la legislación aplicable en materia de **datos personales**, datos contables y datos del sector público, así como de las leyes y reglamentos de control de las exportaciones que pueden limitar la transmisión de determinados datos o programas informáticos a ciertos países. También pueden derivarse de obligaciones contractuales, por ejemplo, de las **licencias de propiedad intelectual** que pueden llegar a exigir que el contenido bajo licencia se aloje en los servidores seguros del propio usuario. Establecer requisitos de **ubicación de los datos** puede resultar deseable por meras razones prácticas, entre ellas, para aumentar la **latencia**, algo especialmente importante en las operaciones en tiempo real como las operaciones bursátiles.

11. El proveedor, en sus condiciones estándar, puede reservarse expresamente el derecho de alojar los datos del cliente en cualquier país en el que operen tanto él como sus subcontratistas. Es muy probable que se siga dicha práctica incluso cuando no exista una disposición de derecho contractual en ese sentido, ya que es algo implícito en la prestación de los **servicios de computación en la nube** que, por regla general, se suministran desde más de un lugar (por ejemplo, las copias de seguridad y la protección antivirus pueden hacerse a distancia remoto y la atención al cliente puede ofrecerse de un modo que permita **aprovechar los husos horarios,** en función del huso horario de cada cliente). El cliente que deba cumplir los requisitos de **ubicación de los datos** podría necesitar que el proveedor le garantizase que es posible cumplir tales requisitos. En los contratos de computación en la nube en los que es posible negociar, podrían incluirse ciertas salvaguardias, como la prohibición de dejar una ubicación especificada o la necesidad de que el proveedor obtenga la autorización previa del cliente para hacerlo [*cross-link*].

- *Requisitos relativos al proveedor*

12. Las posibilidades del cliente de elegir al proveedor más adecuado puede estar limitada, además de por las condiciones del mercado, por disposiciones reglamentarias. Es posible que la ley prohíba celebrar contratos de computación en la nube con proveedores extranjeros, con proveedores de determinadas jurisdicciones o con proveedores que no hayan sido acreditados ante las autoridades competentes del Estado o no hayan recibido certificación de estas. Quizás la ley exija al proveedor extranjero constituir una empresa conjunta con un proveedor nacional u obtener licencias y

permisos locales, como permisos de control a las exportaciones, para poder prestar **servicios de computación en la nube** en una jurisdicción determinada. La elección del proveedor puede verse también afectada por los requisitos relativos a la **ubicación de los datos** [*cross-link*]. A la hora de elegir el proveedor adecuado el cliente también debería tener en cuenta las obligaciones del proveedor previstas en la ley en cuanto a si debe proporcionar acceso a los datos de sus clientes o revelar dichos datos y suministrar alguna otra información a las autoridades de Estados extranjeros.

B. Evaluación precontractual de riesgos

13. Las normas imperativas pueden exigir que se realice una evaluación de riesgos como condición para celebrar un contrato de computación en la nube. Incluso cuando la ley no imponga este requisito, las partes en un contrato de computación en la nube pueden decidir llevar a cabo una evaluación de riesgos que podría ayudarles a determinar cuáles son las medidas más adecuadas para mitigarlos, como la negociación de ciertas cláusulas.

14. No todos los riesgos derivados de los contratos de computación en la nube son específicos de este campo. Algunos de ellos podrían tener que abordarse de forma independiente al contrato de computación en la nube (por ejemplo, los riesgos derivados de las interrupciones en la conexión a Internet), y no todos pueden mitigarse a un coste aceptable (por ejemplo, los daños a la reputación). Además, es posible que la evaluación de riesgos no pueda llevarse a cabo de una sola vez antes de concluir un contrato. Es posible que la evaluación de riesgos se lleve a cabo continuamente durante la vigencia del contrato y que de ello resulte la modificación o resolución de este.

- *Verificación de la información sobre el proveedor elegido*

15. La siguiente información puede ayudar al cliente a ponderar los posibles riesgos de contratar con un determinado proveedor:

a) Las políticas de privacidad, confidencialidad y seguridad del proveedor, en especial en lo que respecta a la prevención de accesos no autorizados, la utilización, la alteración o la destrucción de los datos del cliente durante el tratamiento, el tránsito o la transmisión a los sistemas del proveedor y hacia fuera de ellos;

b) Las garantías ofrecidas al cliente de acceso permanente a los **metadatos**, registros de auditoría y otros registros que demuestren la existencia de medidas de seguridad;

c) La existencia de un plan de recuperación en casos de desastre y las obligaciones de notificación en caso de violación de la seguridad o mal funcionamiento del sistema;

d) El hecho de que el proveedor ofrezca asistencia en los procesos de migración a la nube y finalización del servicio, así como garantías de **interoperabilidad** y **transferibilidad**;

e) Las medidas existentes de investigación de los antecedentes y capacitación de empleados, subcontratistas y otros terceros que participen en la prestación de los servicios de computación en la nube;

f) Las estadísticas de incidentes de seguridad e información sobre la calidad del servicio en anteriores procedimientos de recuperación en casos de desastre;

g) La certificación otorgada por un tercero independiente que acredite el cumplimiento de las normas técnicas;

h) La acreditación de la periodicidad y el alcance de la auditoría realizada por un órgano independiente;

i) La solvencia financiera del proveedor;

j) Las pólizas de seguro contratadas por el proveedor;

k) Los posibles conflictos de intereses; y

l) El alcance de la subcontratación y de los **servicios estratificados de computación en la nube**.

- *Pruebas de penetración, auditorías y visitas sobre el terreno*

16. Las leyes y los reglamentos que el cliente esté obligado a cumplir pueden exigir que se realicen **auditorías**, pruebas de penetración e inspecciones físicas a los centros de datos que prestan los servicios de computación en la nube, especialmente para verificar que su ubicación cumple los requisitos legales sobre **ubicación de los datos**. El cliente y el proveedor tendrían que ponerse de acuerdo sobre las condiciones en que deben llevarse a cabo estas actividades, las fechas en que se realizarían, la distribución de sus costos y la indemnización que se debería pagar en caso de que el proveedor sufriera daños como resultado de esas actividades.

- *Riesgo de que se vulneren derechos de propiedad intelectual*

17. Pueden existir el riesgo de que se vulneren derechos de propiedad intelectual en los casos en los que, por ejemplo, el proveedor no sea el propietario de los recursos que brinda a sus clientes ni quien los ha desarrollado, sino que los utilice en virtud de un acuerdo de **licencia de propiedad intelectual** suscrito con un tercero. También puede surgir dicho riesgo cuando para llevar a efecto lo previsto en el contrato, se exige al cliente que otorgue al proveedor una licencia de uso del contenido que el cliente desee almacenar en la nube. En algunas jurisdicciones, el almacenamiento de contenido en la nube, incluso con el fin de hacer copias de seguridad, puede llegar a considerarse como una reproducción y necesita la autorización previa del propietario de los derechos de propiedad intelectual.

18. Asegurarse de antemano de que la utilización de los servicios de computación en la nube no supondrá una violación de derechos de propiedad intelectual ni una causa de revocación de la licencia concedida a cualquiera de las partes redundará en beneficio de ambas. Los costos de incurrir en una violación de derechos de propiedad intelectual pueden ser muy elevados. Es posible que sea necesario pactar el derecho para conceder sublicencias o celebrar un contrato directo de licencia con el correspondiente tercero licenciante que otorgue el derecho a gestionar las licencias que sean propiedad de terceros. Para utilizar programas informáticos de código abierto u otros contenidos podría ser necesario obtener por anticipado el consentimiento de terceros y revelar el código fuente con las modificaciones introducidas en tales programas y otros contenidos.

- *Riesgos de dependencia tecnológica*

19. Una de las cuestiones más importantes que el cliente debería tener en cuenta es la de evitar o reducir los riesgos asociados a la **dependencia de la solución tecnológica**. Estos riesgos pueden derivarse, en concreto, de la falta de **interoperabilidad** y **transferibilidad**. A menos que el contrato disponga otra cosa, podría ser responsabilidad exclusiva del cliente el crear procedimientos compatibles para la exportación de los datos.

20. El contrato puede incluir la garantía del proveedor sobre la **interoperabilidad** y **transferibilidad** del sistema. Puede exigirse el uso de formatos de exportación de datos y contenidos que sean comunes, ampliamente utilizados y estandarizados o dar al cliente el derecho a elegir entre diferentes formatos. En el contrato se pueden abordar también los derechos del cliente a utilizar productos conjuntos y aplicaciones o programas informáticos del proveedor sin los cuales sería imposible utilizar sus datos y contenidos en otra nube [*cross-link*]. También puede incluirse la obligación del proveedor de prestar asistencia en la exportación de los datos del cliente a sus propios sistemas o a los de otro proveedor en el momento en que extinga el contrato [*cross-link*]. El cliente también debería considerar cuidadosamente el efecto que puede tener la duración del contrato: en los contratos a largo plazo y en aquellos a corto y medio plazo que se renuevan automáticamente puede existir un mayor riesgo de dependencia [*cross-link*].

21. El cliente podría probar de antemano si sus datos y contenidos pueden exportarse a otro proveedor de servicios de nube o a sus propios sistemas y resultar utilizables. También podría ser necesario asegurar la sincronización entre las plataformas internas y en la nube, duplicando sus datos en otro lugar. Una estrategia importante para reducir los riesgos de dependencia puede ser la de contratar con varios proveedores y optar por una combinación de varios tipos de **servicios de computación en la nube** y sus **modelos de despliegue** (por ejemplo, emplear múltiples proveedores).

- *Riesgos de continuidad de las operaciones*

22. El cliente podría querer abordar los riesgos relacionados con la continuidad de las operaciones, no solo en previsión de la fecha fijada para la extinción del contrato, sino también en caso de una posible resolución anticipada, incluso en el supuesto de que alguna de las partes cese en sus actividades comerciales. Los riesgos de continuidad de las operaciones también pueden derivarse de la suspensión de la prestación de los servicios de computación en la nube por parte del proveedor. Es posible que la ley exija al cliente disponer de una estrategia adecuada previamente planificada que le permita garantizar la continuidad de las operaciones y evitar los efectos negativos de la cancelación o la suspensión de los servicios de computación en la nube para los usuarios finales. Algunas cláusulas contractuales pueden ayudar al cliente a reducir los riesgos de continuidad de las operaciones, especialmente en caso de insolvencia del proveedor [*cross-link*] y suspensión o cese unilateral de los servicios de computación en la nube [*cross-link*].

- *Estrategias de salida*

23. El cliente debería examinar con antelación el contenido sujeto a una posible estrategia de salida (por ejemplo, si será necesario retirar únicamente los datos que el cliente ha subido a la nube o también los **datos obtenidos de los servicios de nube**). El cliente podría necesitar también garantías de que tendrá acceso en el momento oportuno a las claves de descifrado custodiadas por el proveedor o por terceros. También debería reflexionar sobre las modificaciones que sería necesario realizar en las **licencias de propiedad intelectual** para permitir el uso de los datos y contenidos fuera del sistema del proveedor. En los casos en que el cliente haya elaborado programas para interactuar directamente con las interfaces de programas de aplicación (API) del proveedor, puede ser necesario volver a escribir dichos programas para tener en cuenta las nuevas API del proveedor. Los clientes de servicios **SaaS** con una importante base de usuarios quizás deban incurrir en costos de cambio especialmente elevados en el momento en que decidan migrar a otro proveedor de **SaaS**, ya que podría ser necesario formar de nuevo a los usuarios finales.

24. Todos estos factores, además del tiempo necesario para exportar todos los datos y contenidos del cliente y hacer que estén plenamente disponibles en sus propios sistemas o en los de otro proveedor, deben tenerse en cuenta a la hora de negociar las cláusulas del contrato relativas a la financiación del servicio [*cross-link*].

C. Otros aspectos precontractuales

- *Revelación de información*

25. Es posible que la legislación aplicable exija que las partes de un contrato se suministren recíprocamente información que les permita tomar una decisión fundamentada sobre la celebración del contrato. En algunas jurisdicciones, la falta de una comunicación clara a la otra parte de la información necesaria para que las obligaciones de esa parte queden o sean susceptibles de quedar determinadas antes de la firma del contrato puede hacer que dicho contrato, o una parte de este, resulte nulo de pleno derecho o que la parte perjudicada pueda reclamar una indemnización por daños y perjuicios.

26. En algunas jurisdicciones, la información precontractual puede considerarse parte integrante del contrato. En tales casos, las partes deberían asegurarse de que esa información sea debidamente registrada y evitar cualquier discrepancia entre dicha información y el propio contrato. Es posible que las partes tengan que ocuparse también de cuestiones relacionadas con los efectos de la revelación precontractual de información sobre la flexibilidad y la innovación en la etapa de ejecución del contrato.

- *Confidencialidad*

27. Es posible que parte de la información revelada en la fase previa al contrato sea considerada como confidencial (por ejemplo, los datos de seguridad, identificación y autentificación exigidos por el cliente u ofrecidos por el proveedor, la información acerca de los subcontratistas o de la ubicación y el tipo de los centros de datos, que podría hacer que se identificara el tipo de datos almacenados en ellos y permitir el acceso a esos datos a las autoridades del Estado, incluso de Estados extranjeros). Las partes en un futuro contrato tal vez necesiten llegar a un acuerdo sobre la confidencialidad de la información que se revelaría en la fase precontractual. Tal vez también necesiten firmar acuerdos de confidencialidad o contratos de no divulgación con los terceros que participen en el proceso de reunión de información antes de la celebración del contrato, en ejercicio de la diligencia debida (por ejemplo, los auditores).

- *Migración a la nube*

28. Antes de migrar datos a la nube suele pedirse al cliente que clasifique los datos que va a migrar y los asegure en función de su grado de importancia y confidencialidad, informando al proveedor sobre el nivel de protección necesario para cada tipo de datos. Es posible que el cliente deba también proporcionar al proveedor otro tipo de información necesaria para la prestación de los servicios (como el plan de conservación y eliminación de los datos del cliente, la identidad del usuario y los mecanismos y procedimientos de gestión de acceso para acceder a las claves de cifrado si fuera necesario).

29. Además de la transferencia de datos y contenidos desde los sistemas del cliente o desde su proveedor anterior a la nube del nuevo proveedor, la migración a la nube puede entrañar pruebas de instalación, configuración y cifrado y la formación del personal del cliente y otros usuarios finales. El proveedor puede ayudar al cliente con esas cuestiones a cambio del pago de honorarios adicionales u otro tipo de remuneración, en el marco del contrato firmado con el cliente o en virtud de un contrato independiente suscrito con él o con un tercero que actúe en su nombre (por ejemplo, un **integrador de sistemas**). Las partes que participen en la migración deben ponerse de acuerdo sobre sus funciones y responsabilidades en lo que respecta a la instalación y la configuración, el formato en que migrarán los datos o contenidos a la nube, el calendario de la migración, el procedimiento de aceptación que garantice que la migración se llevó a cabo conforme a lo acordado y otros detalles del plan de migración.

Segunda parte. La redacción del contrato

A. Consideraciones generales

- *Libertad de contratación*

30. El principio ampliamente reconocido de la libertad de contratación en las operaciones comerciales permite a las partes celebrar contratos y pactar su contenido. Las disposiciones legislativas sobre las cláusulas no negociables aplicables a determinados tipos de contrato o las normas que penalizan el abuso del derecho o las conductas que afectan al orden público, ofenden la moral, etc., pueden imponer ciertas restricciones a la libertad de contratación. Las consecuencias del incumplimiento de estas restricciones pueden ir desde privar de exigibilidad al contrato, o a una de sus partes a que las partes incurran en responsabilidad civil, administrativa o penal. La posibilidad de exigir el cumplimiento de los contratos que no han sido negociados libremente, especialmente aquellos que imponen condiciones abusivas a la parte más débil en la negociación [*cross-link*], puede resultar discutible en las jurisdicciones en las que las partes deben respetar el principio de la buena fe negocial.

- *La formación del contrato*

31. Los conceptos de oferta y aceptación se han utilizado tradicionalmente para determinar si las partes han llegado o no a un acuerdo sobre los respectivos derechos y obligaciones que les vincularán durante el plazo de vigencia de dicho contrato y cuándo lo han hecho. La legislación aplicable puede exigir que se cumplan ciertas condiciones para que la propuesta de celebrar un contrato se considere una oferta definitiva y vinculante (por ejemplo, la propuesta debe ser suficientemente precisa en lo que respecta a los servicios de computación en la nube y a las condiciones de pago).

32. El contrato se considera celebrado cuando se acepta la oferta. Puede haber diferentes mecanismos de aceptación (por ejemplo, en el caso del cliente, puede ser suficiente marcar una casilla de una página web, registrarse en un servicio de computación en la nube en línea, comenzar a utilizar los servicios de computación en la nube o pagar un precio por los servicios; en el caso del proveedor, puede bastar con empezar a prestar los servicios o continuar haciéndolo; y, para ambas partes, la firma de un contrato en línea o en papel). Los cambios sustanciales en la oferta (por ejemplo, los referidos a la responsabilidad, la calidad y la cantidad de los servicios de computación en la nube que han de prestarse o a las condiciones de pago) pueden considerarse como una contraoferta que tendría que ser aceptada por la otra parte para que el contrato se considerase celebrado.

33. Por regla general, las **soluciones de nube genéricas y estandarizadas para múltiples suscriptores** se ofrecen mediante aplicaciones interactivas (por ejemplo, los contratos electrónicos de tipo *click-wrap*). En estos casos, no existe apenas margen para la negociación y modificación de la oferta estándar. Hacer clic en “acepto”, “OK” o “de acuerdo” es el único paso necesario para celebrar el contrato. En los casos en los que se negocia el contrato, su formación puede consistir en una serie de acciones, entre las que destacan el intercambio de información preliminar, las negociaciones entre las partes, la entrega y aceptación de una oferta y la redacción del contrato.

- *La forma del contrato*

34. Los contratos de computación en la nube suelen firmarse en línea. Pueden recibir diferentes denominaciones (contrato de servicios de computación en la nube, contrato marco de servicios o condiciones de servicio) y pueden incluir uno o más documentos tales como una **política de uso aceptable** (AUP, por sus siglas en inglés), un **acuerdo sobre las características de los servicios** (**SLA**, por sus siglas en inglés), un acuerdo de procesamiento de datos o política de protección de datos, una política de seguridad y contrato de licencia.

35. Las normas jurídicas aplicables a los contratos de computación en la nube pueden exigir que el contrato conste **por escrito** (especialmente cuando incluye **el procesamiento de datos personales**) y que se adjunten al contrato principal todos los documentos incorporados por referencia. Incluso en los casos en los que no se exige la forma **escrita**, las partes pueden optar por celebrarlo de esta manera incorporando, asimismo, todos los acuerdos complementarios, para facilitar la consulta y mejorar la claridad, la integridad, la exigibilidad y la eficacia del contrato.

36. En algunas jurisdicciones, la ley aplicable puede exigir que el contrato se firme en papel, por ejemplo, por motivos fiscales.

- *Definiciones y terminología*

37. Los contratos de computación en la nube podrían contener numerosos términos técnicos que, por la naturaleza de los **servicios de computación en la nube** que regulan, pueden resultar necesarios. Se puede incluir en el contrato un glosario que incluya estos términos, así como las definiciones de los principales términos empleados a lo largo de todo el contrato a fin de evitar ambigüedades en su interpretación. Las partes deberían considerar la posibilidad de utilizar la terminología establecida internacionalmente a fin de garantizar la coherencia y la claridad jurídica.

- *Contenido mínimo del contrato*

38. Normalmente, el contrato debería incluir la siguiente información: a) identificación de las partes; b) definición de su objeto y su ámbito de aplicación; c) descripción de los derechos y obligaciones de las partes, como las condiciones de pago; d) su plazo de vigencia y las condiciones para su extinción o renovación; y también e) las acciones de reparación disponibles en caso de incumplimiento y las eximentes de responsabilidad. También es habitual incluir cláusulas de resolución de controversias, de elección de la legislación aplicable y de jurisdicción competente.

B. Identificación de las partes

39. Identificar correctamente a las partes contratantes puede tener un efecto directo sobre la formación y la exigibilidad del contrato. Para pueda corroborarse la personalidad jurídica de una entidad mercantil (ya sea que se trate de una empresa o de un particular) y su capacidad para obligarse contractualmente suele ser suficiente con incluir el nombre de dicha persona jurídica, su forma legal, su número de inscripción en el registro (si procede) y su domicilio social o dirección de negocio, junto con la mención de sus documentos fundacionales. La ley puede exigir que se incluya información adicional, por ejemplo, un número de identificación fiscal o un poder de representación que acredite las facultades de la persona física que firma para obligarse en nombre de la persona jurídica.

40. Es posible verificar la identidad de la persona jurídica de diferentes formas y pueden hacerlo las partes directamente o puede hacerlo un tercero. Normalmente, las partes disponen de libertad para decidir los métodos de identificación, salvo que se lo impida la legislación aplicable. Puede ser necesaria la presencia física del representante autorizado de la persona jurídica, o puede ser suficiente que esté presente en remoto mediante medios electrónicos de identificación que resulten aceptables para las partes. En los casos en los que las partes pueden elegir, su elección suele venir determinada por varios factores, como los riesgos que implica cada negociación contractual. Algunas legislaciones pueden exigir o reconocer solo algunos métodos de identificación, en especial en los casos en los que se utilice un poder de representación. También pueden exigir al proveedor que identifique a sus clientes ante las autoridades competentes del Estado, de conformidad con las normas aplicables.

C. Definición del objeto y ámbito de aplicación del contrato

41. El objeto de los contratos de computación en la nube varía sustancialmente en lo que se refiere a su tipología y complejidad, dado que existe una gran variedad de **servicios de computación en la nube**. Dentro del período de vigencia de un mismo contrato su objeto puede variar: algunos **servicios de computación en la nube** podrán cancelarse y otros podrán añadirse. El objeto del contrato puede incluir la prestación de servicios esenciales, auxiliares y opcionales.

42. La descripción del objeto del contrato podría incluir la descripción del tipo de servicios de computación en la nube (**SaaS**, **PaaS**, **IaaS** o una combinación de todos ellos), su **modelo de despliegue** (**público,** compartido**, privado** o **híbrido**) y sus características técnicas, de calidad y funcionales, así como las normas aplicables. Algunos de los documentos incluidos en el contrato pueden resultar pertinentes a la hora de determinar su objeto [*cross-link*].

- *Acuerdo sobre las características de los servicios (SLA)*

43. El **acuerdo sobre las características de los servicios (SLA)** incluye **parámetros de desempeño** que sirven para evaluar los servicios de computación en la nube prestados por el proveedor. Por ello, resulta una herramienta importante a la hora de determinar el alcance de las obligaciones contractuales y los posibles incumplimientos del proveedor. Los **SLA** estandarizados pueden no prever obligaciones de resultado específicas y contener en su lugar declaraciones de intención cuyo cumplimiento no puede exigirse (por ejemplo, “el proveedor hará todo lo que esté [razonablemente] a su alcance para garantizar una alta disponibilidad del servicio”, “el proveedor procurará por mantener los servicios disponibles las 24 horas del día, 7 días a la semana [o que el período de disponibilidad del servicio alcance el 99%], pero sin garantizarlo”). En estos acuerdos, el cliente quizás no disponga de ningún recurso contra el proveedor, ya que las cláusulas que establecen obligaciones de medios pueden resultar ambiguas. Para evitar estas situaciones, el cliente podría incluir en el **SLA** parámetros de desempeño cuantitativos y cualitativos con formas de evaluación concretas, garantías de calidad y una metodología para evaluar el desempeño.

Ejemplos de parámetros de desempeño cuantitativos

Capacidad	- X capacidad de almacenamiento de datos - X memoria disponible para el programa en ejecución
Disponibilidad	- Cantidad o porcentaje de **período de disponibilidad del servicio** (por ejemplo, el 99,9%) - Fórmula detallada para calcular el **período de disponibilidad** - Fechas concretas o días y horas en los que la disponibilidad del servicio resulta crítica (100%) - Disponibilidad de una aplicación concreta (100%)
Período de interrupción o cortes del servicio	- 10 cortes de 6 minutos - 1 corte de 1 hora - Tiempo para recuperar los datos tras un corte del servicio
Elasticidad y escalabilidad	- en qué medida y con qué rapidez se puede aumentar o reducir la escalabilidad de los servicios (por ejemplo, cuál es la disponibilidad máxima de los recursos en un plazo mínimo)
Latencia	- Inferior a X milisegundos

Cifrado	- Valor de X bits en reposo, en tránsito y en uso
Servicios de apoyo	- 24/7 - Horario habitual de actividad del cliente
Gestión de desastres e incidentes y planes de recuperación de material	- Tiempo máximo de resolución de incidentes - **Tiempo** máximo **de respuesta inicial** - **Objetivos de punto de recuperación** (**RPO**, por sus siglas en inglés). - **Objetivos de punto de recuperación** (**RTO**, por sus siglas en inglés). - Fechas o días y horas concretos en que resulta fundamental conseguir la recuperación de material en un plazo X
Permanencia del almacenamiento de datos	- Datos intactos / (datos intactos + datos perdidos durante un período de tiempo X (por ejemplo, un mes natural). Convendría definir el tipo de datos (por ejemplo, archivos, bases de datos, códigos, aplicaciones) y las unidades de medida (el número de archivos, la longitud de bits).

Ejemplos de parámetros de desempeño cualitativos

Portabilidad de los datos	- El cliente puede recuperar sus datos mediante un único enlace de descarga o una API documentada - El formato de los datos está suficientemente estructurado y documentado para permitir que el cliente lo reutilice o lo reestructure, si se quiere, en un formato diferente
Requisitos de **ubicación de los datos**	- Los datos del cliente (incluidas todas sus copias, los **metadatos** y sus copias de seguridad) se almacenan exclusivamente en centros de datos ubicados físicamente en las jurisdicciones que se indican en el contrato y son propiedad y están gestionados por entidades radicadas en tales jurisdicciones. — Los datos nunca son trasladados fuera del país X, deben duplicarse en el país Y, así como en otros países, pero nunca en el país Z.
Seguridad	- Un auditor independiente certifica los servicios previstos en el contrato al menos una vez al año, verificando el cumplimiento de una norma de seguridad recogida en el propio contrato
Cifrado	- El proveedor se asegurará de que se cifren los datos del cliente cada vez que sean transportados por una red de comunicaciones pública, como Internet, para ser enviados tanto desde el cliente al proveedor como entre los centros de datos utilizados por el proveedor, así como cuando estén en reposo en los centros de datos del proveedor - El proveedor ha aplicado una política de gestión de claves en cumplimiento de una norma internacional indicada en el contrato

Protección o privacidad de los datos	- Un auditor independiente certifica los servicios previstos en el contrato al menos una vez al año verificando la aplicación de una norma de protección o privacidad que figura en el propio contrato
Eliminación de datos	- El proveedor garantiza que los datos del cliente se eliminen de forma efectiva, irrevocable y permanente cuando este lo solicite, en un plazo determinado establecido en el contrato y cumpliendo la norma o la técnica allí señaladas.

44. El contrato podría incluir mecanismos para facilitar la aplicación de los cambios solicitados por el cliente. De otro modo, cada vez que el cliente solicitara un cambio habría que pasar por un prolongado proceso de negociación.

Evaluación del desempeño

45. Es posible que sea necesario incluir en el contrato ciertas disposiciones sobre los procedimientos y la metodología elegidos para la evaluación de los servicios, especificando, en particular, un período de referencia para hacerlo (diario, semanal, mensual), sobre los mecanismos de información acerca de la prestación de los servicios (frecuencia y forma), sobre el papel y las obligaciones de las partes y sobre el punto de medición. Las partes pueden pactar una evaluación independiente del desempeño y la distribución de sus costos asociados.

46. Al cliente le podría interesar que se evaluaran los servicios en las horas de máxima intensidad de tráfico, es decir, cuando son más necesarios. El cliente quizás pueda verificar algunas evaluaciones del proveedor o de terceros, pero solo las evaluaciones del desempeño en el punto de consumo, no las evaluaciones del desempeño del sistema en el punto de prestación del servicio. El cliente tal vez pueda evaluar estas últimas a partir de los informes facilitados por el proveedor o por terceros. El proveedor podría convenir en proporcionar al cliente informes de desempeño cuando este último lo solicite, de una forma periódica (diaria, semanal, mensual, etc.) o cuando se produzca un determinado incidente. Como alternativa a lo anterior, el proveedor puede conceder al cliente el derecho a revisar sus registros de las evaluaciones del nivel de servicio. Algunos proveedores permiten que el cliente compruebe los datos de nivel de servicio en tiempo real.

47. El contrato puede disponer que alguna de las partes o ambas conserven durante un tiempo determinado los registros correspondientes a la prestación o al consumo de los servicios. Esta información puede resultar útil a la hora de negociar modificaciones al contrato y en caso de que surjan controversias entre las partes.

- *La política de uso aceptable (AUP)*

48. La **AUP** fija las condiciones de uso por parte del cliente y sus usuarios finales de los servicios de computación en la nube que figuran en el contrato. Su finalidad es la de proteger al proveedor frente a la posible responsabilidad derivada de la actividad de sus clientes y los usuarios finales de estos últimos. Se espera que los clientes acepten esta política, que formará parte del contrato con el proveedor. La inmensa mayoría de las normas de la AUP prohíben un conjunto de actividades que el proveedor considera constituyen usos inadecuados o ilícitos de los **servicios de computación en la nube**. En algunos casos puede estar justificado eliminar ciertas prohibiciones teniendo en cuenta las necesidades concretas del cliente.

49. Es habitual que el proveedor exija el cumplimiento de la **AUP** a los usuarios finales del cliente y que obligue a este último a hacer todo lo posible, incluso en el plano comercial, para garantizar dicho cumplimiento. Algunos proveedores pueden exigir que los clientes impidan proactivamente todo uso no autorizado o inadecuado por parte de terceros de los servicios de computación en la nube que figuran en el contrato. El cliente tal vez prefiera limitar sus obligaciones de comunicación previstas en la **AUP** a los usuarios finales conocidos y no autorizar o permitir deliberadamente tales usos, además de notificar al proveedor todo uso no autorizado o inadecuado del que tenga conocimiento.

- *Política de seguridad*

50. Mantener la seguridad del sistema, y de los datos del cliente, significa que el proveedor y el cliente deberán compartir responsabilidades. Se debería especificar en el contrato las funciones y las responsabilidades de cada parte en lo que respecta a las medidas de seguridad, para reflejar las obligaciones que la ley imponga a alguna de las partes o a ambas.

51. Es habitual que el proveedor siga sus políticas de seguridad. En algunas situaciones podría negociarse que el proveedor aceptase las políticas de seguridad del cliente, aunque no en el caso de las **soluciones de nube genéricas y estandarizadas para múltiples suscriptores**. En el contrato pueden detallarse las medidas de seguridad que han de adoptarse (por ejemplo, los requisitos para el saneamiento o la eliminación de los datos almacenados en un soporte dañado, el almacenamiento de diferentes paquetes de datos en diferentes ubicaciones o el almacenamiento de los datos del cliente en un equipo físico concreto exclusivo para ese cliente). No obstante, las partes deberán ponderar el riesgo de incluir una cantidad excesiva de información de seguridad en el contrato.

52. Algunas medidas de seguridad quizás no impliquen la actuación de una de las partes y dependan exclusivamente de las actividades ordinarias de la otra, como las inspecciones llevadas a cabo por el proveedor en el equipo físico en el que se almacenan los datos y en el que se ejecutan los servicios, así como las medidas eficaces para garantizar el control del acceso a dichos equipos. En otros casos, el hecho de permitir que una de las partes cumpla con sus correspondientes deberes o evalúe y controle la calidad de las medidas de seguridad puestas en marcha puede hacer necesaria la actuación de la otra parte. El cliente podría estar obligado, por ejemplo, a actualizar las listas con las credenciales de los usuarios y sus derechos de acceso, e informar puntualmente al proveedor de los cambios que se realicen para garantizar el correcto funcionamiento de los mecanismos de gestión de identidad y acceso. El cliente también podría tener que indicar al proveedor el nivel de seguridad que debe aplicarse a cada una de las categorías de datos.

53. Es posible que algunas amenazas de seguridad queden fuera del marco contractual pactado entre el cliente y el proveedor, y quizás hagan necesario que las condiciones del contrato de computación en la nube se armonicen con las recogidas en otros contratos suscritos por ambas partes (como las que se firman con proveedores de servicios de Internet).

- *Integridad de los datos*

54. Los contratos estandarizados de los proveedores pueden incluir cláusulas de descargo general de responsabilidad, en que se señale que, en última instancia, la responsabilidad de preservar la integridad de los datos del cliente sea del propio cliente. En ocasiones los proveedores tan solo garantizan, de una forma no vinculante, que harán todo lo que esté en sus manos para proteger los datos del cliente.

55. Algunos proveedores aceptan asumir ciertos compromisos relativos a la integridad de los datos (como realizar copias de seguridad con regularidad), en ocasiones a cambio de un pago adicional. Con independencia de lo pactado con el proveedor, el cliente podría valorar si es necesario garantizar el acceso a al menos una de las copias utilizables de sus datos que se encuentren fuera del control, el alcance o la influencia del proveedor y sus subcontratistas y en la que estos no tengan participación.

- *Cláusula de confidencialidad*

56. En algunos casos, el proveedor no ofrece incluir una cláusula de confidencialidad o de no divulgación, o tales cláusulas no son suficientes para garantizar la confidencialidad de los datos del cliente. Algunos proveedores incluso quizás rechacen expresamente asumir cualquier obligación de confidencialidad respecto de los datos del cliente, trasladando a este último toda la responsabilidad de mantener la confidencialidad de sus datos mediante el uso de sistemas como el cifrado. Es posible que los proveedores solo acepten asumir la obligación de mantener la confidencialidad de los datos revelados por el cliente durante las negociaciones contractuales, pero no la de los datos procesados durante la prestación del servicio. La disposición del proveedor para comprometerse a garantizar la confidencialidad de los datos del cliente podría depender de la naturaleza de los servicios que deban prestarse a este con arreglo a las cláusulas del contrato y, en especial, de si el proveedor deberá o no tener acceso no cifrado a los datos para la prestación de tales servicios.

57. En la mayoría de los casos, el cliente querrá que el proveedor garantice la confidencialidad de todos sus datos alojados en la nube y se comprometa a asumir un mayor nivel de confidencialidad en relación con algunos datos sensibles (con un régimen de responsabilidad diferente ante una posible violación de la confidencialidad de dichos datos). Al cliente pueden preocuparle especialmente sus secretos comerciales, sus conocimientos especializados y aquella información que es necesario mantener en secreto por disposición legal o debido a compromisos asumidos con terceros.

58. En los casos en los que es necesario emplear un nivel adicional de protección, tal vez convenga restringir el acceso a los datos del cliente a un número limitado de personas dentro de la plantilla del proveedor y exigir a este último que obtenga de tales personas compromisos individuales de confidencialidad, en especial de aquellas que desempeñan funciones de alto riesgo (por ejemplo, los administradores del sistema, los auditores y las personas que se ocupan de la detección de intrusos y de responder a incidentes). Correspondería al cliente el especificar correctamente al proveedor la información confidencial, el nivel necesario de protección, la legislación aplicable o los requisitos contractuales y todos los cambios que afecten a esa información, como los cambios que se produzcan en la legislación aplicable.

59. En algunos casos, puede resultar necesario revelar los datos del cliente para cumplir lo pactado en el contrato. En otros, la revelación puede constituir una exigencia legal, por ejemplo, cuando existe el deber de aportar información a las autoridades estatales competentes [*cross-link*]. En tales casos estarían justificadas las ciertas excepciones a las cláusulas de confidencialidad.

60. A cambio, el proveedor puede solicitar que el cliente asuma la obligación de no revelar la información relativa a las medidas de seguridad del proveedor, así como otros detalles del servicio que este presta al cliente conforme a su contrato o a lo previsto en la ley.

- *Protección de datos, política de privacidad o acuerdo de procesamiento de datos*

61. Los **datos personales** son objeto de una protección legal especial en muchas jurisdicciones. La legislación aplicable al **procesamiento** de dichos datos puede ser diferente a la que se aplica al contrato y, en ese caso, invalidará las cláusulas contractuales no conformes con dicha legislación.

62. El contrato puede incluir una cláusula de protección de datos o de privacidad, un acuerdo de procesamiento de datos o de un tipo similar, aunque quizás algunos proveedores solo acepten la obligación general de cumplir la legislación vigente en materia de protección de datos. En algunas jurisdicciones es posible que no baste con este compromiso general: el contrato debería contener, como mínimo, su objeto, su duración, la naturaleza y la finalidad del **procesamiento**, el tipo de **datos personales** que han de recogerse y las categorías de los **sujetos de los datos**, así como los derechos y las obligaciones del **responsable de los datos** y del **procesador de los datos**. Cuando no existe la posibilidad de negociar la inclusión en el contrato de una cláusula de protección de datos, el cliente tal vez necesite al menos revisar las condiciones estándar

para saber si dichas disposiciones le conceden las garantías suficientes de que el **procesamiento de los datos personales** se realizará de acuerdo con la ley y que dispone de los mecanismos adecuados para solicitar una indemnización por daños y perjuicios.

63. Es probable que el propio cliente sea también el **responsable de los datos** y asuma la obligación de cumplir la legislación sobre protección de **datos personales** recopilados y procesados en la nube. El cliente quizás procure incluir cláusulas contractuales que obligarían al proveedor a colaborar con el cliente para que este último pueda cumplir la normativa aplicable en materia de protección de datos como las peticiones relativas a los **derechos de los sujetos de los datos**. Podrían negociarse medidas de compensación por separado en el caso de que el proveedor incumpliera esta obligación, como la posibilidad de que el cliente resolviera unilateralmente el contrato y de que exigiera el pago de una indemnización por daños y perjuicios del proveedor.

64. En los contratos estandarizados de los proveedores suele estipularse que estos no asumen la función de **responsable de los datos**. Es probable que el proveedor solo actúe como **procesador de los datos** cuando procese los datos del cliente siguiendo sus instrucciones con el único fin de proporcionar los servicios de computación en la nube. No obstante, y con independencia de lo pactado en el contrato, el proveedor puede ser considerado el **responsable de los datos** cuando además procese los datos para sus propios fines o siguiendo las instrucciones de las autoridades del Estado [*cross-link*]. En tales casos, asumirá la plena responsabilidad de la protección de **datos personales** por dicho **procesamiento**.

- *Obligaciones derivadas de las violaciones de los datos y otros incidentes de seguridad*

65. Tanto la ley como las cláusulas del contrato, o ambas, pueden obligar a las partes a que se notifiquen mutuamente y de inmediato la producción de un incidente de seguridad de importancia para el contrato o cualquier sospecha que tengan sobre la producción de un posible incidente. Esta obligación puede existir con independencia de la obligación general exigida por ley de notificar a todas las partes interesadas (como los **sujetos de los datos**, las compañías de seguros y las autoridades del Estado) acerca de los incidentes de seguridad que se produzcan a fin de evitar o reducir al mínimo sus efectos.

66. Las partes podrán pactar el plazo de notificación (por ejemplo, un día después de que la parte haya tenido conocimiento del incidente o la amenaza), la forma y el contenido de la **notificación del incidente de seguridad** y las **medidas posteriores a los incidentes**, que pueden variar en función de las categorías de los datos almacenados en la nube. Los requisitos de notificación deberían tener en cuenta la necesidad de no revelar información confidencial que pudiera poner en riesgo los sistemas, la red o las operaciones de la parte afectada.

67. El cliente podría querer reservarse el derecho a resolver el contrato en caso de que se produjera un incidente de seguridad grave que tuviera como consecuencia, por ejemplo, la pérdida de sus datos.

D. Derechos sobre los datos del cliente y otros contenidos

- *Derechos del proveedor sobre los datos del cliente necesarios para la prestación de los servicios*

68. Los proveedores suelen reservarse el derecho de acceder a los datos del cliente para cumplir con el principio de la "necesidad de saber". Esto permite que los empleados y subcontratistas del proveedor, y otros terceros (por ejemplo, los auditores), tengan acceso a los datos del cliente cuando sea necesario para la prestación de los servicios de computación en la nube (con fines de mantenimiento, soporte y seguridad, por ejemplo) y para supervisar el cumplimiento de los correspondientes acuerdos de **AUP, SLA y de las licencias de propiedad intelectual**, así como otros documentos contractuales. Al cliente puede interesarle, no obstante, reducir el número de situaciones en las cuales se

permita este acceso e insistir en que se utilicen medidas que garanticen la confidencialidad y la integridad de sus datos.

69. Cuando el cliente solicita al proveedor un determinado servicio o una determinada funcionalidad puede considerarse que concede implícitamente a este último ciertos derechos para acceder a sus datos, sin los cuales el proveedor no podría prestar tales servicios. Por ejemplo, si el proveedor tiene la obligación de realizar periódicamente copias de seguridad de los datos del cliente, el cumplimiento de esa tarea exige disponer del derecho a hacer copias de los datos. Del mismo modo, si los subcontratistas deben manipular los datos del cliente, el proveedor debe tener la posibilidad de transferir los datos a los subcontratistas.

70. En el contrato puede indicarse expresamente cuáles son los derechos sobre los datos que el cliente otorga al proveedor y que son necesarios para el cumplimiento del contrato, en qué casos y en qué medida el proveedor puede transferir esos derechos a terceros (por ejemplo, a sus subcontratistas) y el ámbito geográfico y temporal de los derechos concedidos expresa o implícitamente. Las limitaciones geográficas podrían ser especialmente importantes para el cliente si este desea impedir que sus datos salgan de un determinado país o región. Asimismo, normalmente el contrato también indicaría si el cliente tiene la facultad de revocar los derechos otorgados expresa o implícitamente y en qué condiciones. Dado que la capacidad de prestar los servicios con el nivel de calidad exigido puede depender de los derechos otorgados por el cliente, la revocación de ciertos derechos puede tener como consecuencia directa la modificación o resolución del contrato.

- *Utilización de los datos del cliente por parte del proveedor para otros fines*

71. El proveedor puede solicitar la utilización de los datos del cliente para otros fines distintos a los relacionados con la prestación de los servicios de computación en la nube previstos en el contrato (para fines publicitarios, de generación de estadísticas, de elaboración de informes analíticos o de pronósticos, de participación en otras prácticas de extracción de datos, etc.). En tales casos, el cliente debe tener en cuenta: a) qué información del cliente y sus usuarios finales se recopilará y cuáles son los motivos y fines de su recopilación y uso por parte del proveedor; b) si esa información se va a compartir con otras organizaciones, empresas o particulares y, de ser así, por qué motivo y si esto se llevará a cabo con o sin el consentimiento del cliente; y c) de qué manera se va a garantizar el cumplimiento de las políticas de confidencialidad y seguridad si el proveedor comparte esa información con terceros. Además, en los casos en que la utilización por el proveedor de los datos del cliente afecte a **datos personales**, las partes deberían evaluar cuidadosamente sus respectivas obligaciones de cumplir lo previsto en las leyes de protección de datos.

72. En general, el contrato debería indicar que el proveedor no adquiere automáticamente ningún derecho a utilizar los datos del cliente para sus propios fines. En el contrato se pueden enumerar, no obstante, las circunstancias en las cuales puede resultar admisible utilizar los datos del cliente para fines distintos a la prestación de los servicios. Por ejemplo, el contrato podría establecer que el proveedor pueda utilizar los datos para sus propios fines durante el plazo de vigencia del contrato o después de ese plazo, pero como datos abiertos y anónimos o de forma agregada y sin identificar. En tales casos, el contrato puede establecer la obligación de que los datos del cliente se utilicen de forma que sean anónimos o no permitan identificar a los usuarios a fin de garantizar el cumplimiento de las normas vigentes en materia de protección de datos, entre otras. El contrato también puede imponer límites a la reproducción del contenido y a la comunicación pública.

- *Utilización por parte del proveedor del nombre, logotipo y marcas del cliente*

73. Las condiciones estándar de los proveedores pueden conceder a estos el derecho a utilizar los nombres, los logotipos y las marcas del cliente en su propia publicidad. El cliente puede negociar la supresión o la modificación de esas disposiciones. Por ejemplo, puede exigir que el proveedor solicite su autorización previa para poder utilizar el nombre del cliente, sus logotipos y sus marcas o puede limitar el uso permitido de su nombre.

- *Actuaciones del proveedor relativas a los datos del cliente tras recibir un requerimiento del Estado o para cumplir la normativa vigente*

74. Las condiciones estándar del proveedor pueden concederle una amplia discrecionalidad para revelar los datos del cliente, o proporcionar acceso a estos a las autoridades del Estado (y podrían incluir, por ejemplo, una expresión del siguiente tenor o de un tenor similar: "cuando hacerlo sea en el interés superior del proveedor"). Al cliente podría interesarle limitar los supuestos en los que el proveedor pueda actuar de este modo, como cuando reciba una orden de un tribunal u otra autoridad del Estado instándole a facilitar el acceso a los datos, suprimirlos o modificarlos (por ejemplo, cuando los **sujetos de los datos** quieren ejercer su **derecho** al olvido). Sin embargo, el proveedor podría insistir en su derecho a eliminar o bloquear de inmediato los datos del cliente en otros supuestos, independientemente de que exista o no una orden del Estado a fin de evitar su responsabilidad legal, por ejemplo, cuando el proveedor tenga conocimiento de la existencia de contenido ilícito (procedimiento de "notificación y retirada" [*cross-link*]).

75. En el contrato se puede establecer, como mínimo, que el proveedor está obligado a notificar de inmediato al cliente de la existencia de una orden del Estado o sus propias decisiones en lo que respecta a los datos del cliente, incluyendo en la notificación una descripción de los datos de que se trate, salvo que realizar dicha notificación constituya una violación de la ley. Cuando no sea posible realizar la notificación ni dar intervención al cliente por adelantado, el contrato puede exigir que el proveedor notifique de esa información al cliente inmediatamente después. El contrato puede obligar al proveedor a llevar un registro de las órdenes, solicitudes y demás actividades relacionadas con los datos del cliente, y conceder a este último acceso a ese registro.

- *Derechos sobre los datos obtenidos de los servicios de nube*

76. Tal vez sea necesario incluir en el contrato ciertas disposiciones relativas a los derechos del cliente sobre los **datos obtenidos de los servicios de nube** y sobre la forma de ejercitar esos derechos durante la vigencia de la relación contractual y tras su extinción.

- *Cláusula de protección de los derechos de propiedad intelectual*

77. Algunos tipos de contratos de computación en la nube pueden hacer nacer derechos de propiedad intelectual, ya sea conjuntamente para el proveedor y el cliente (por ejemplo, las mejoras de los servicios derivadas de las sugerencias del cliente) o solo para el cliente (nuevas aplicaciones, programas informáticos y otros trabajos originales). El contrato puede incluir una cláusula expresa de propiedad intelectual que disponga a cuál de las partes en el contrato pertenecen los derechos sobre los objetos desplegados o desarrollados en la nube, y cómo pueden las partes usarlos. Cuando no exista la posibilidad de negociar este aspecto, el cliente debería poder revisar, al menos, las cláusulas de propiedad intelectual a fin de determinar si el proveedor le ofrece suficientes garantías y le permite disponer de los instrumentos necesarios para proteger y ejercitar sus derechos de propiedad intelectual, evitando los riesgos de **dependencia** [*cross-link*].

- *Recuperación de datos con una finalidad jurídica*

78. Los clientes pueden necesitar buscar y encontrar datos alojados en la nube en su formato original con una finalidad jurídica, por ejemplo, en el marco de un proceso judicial. Más específicamente, los registros electrónicos deberían poder cumplir las normas de auditoría e investigación. Algunos proveedores quizás puedan ofrecer asistencia a los clientes para llevar a cabo la recuperación de los datos en el formato exigido por la ley con una finalidad jurídica. En esos casos, el contrato debería establecer exactamente qué asistencia el cliente necesitaría recibir por parte del proveedor para cumplir las órdenes de las autoridades competentes relativas a la recuperación de datos con una finalidad jurídica.

- *Eliminación de datos*

79. La eliminación de los datos plantea cuestiones que deben ser tenidas en cuenta durante toda la vigencia del contrato y muy especialmente en el momento de su extinción. Por ejemplo, es posible que ciertos datos deban eliminarse siguiendo el plan de retención del cliente. Los datos sensibles pueden tener que ser destruidos en un momento determinado de su ciclo de vida (por ejemplo, mediante la destrucción de los discos duros al finalizar la vida útil del equipo que almacenaba esos datos). También es posible que resulte necesario eliminar los datos para cumplir un mandamiento legal de eliminación o cuando se confirme que se han vulnerado derechos de propiedad intelectual [*cross-link*].

80. Las cláusulas estándar del proveedor podrían contener afirmaciones que no fueran vinculantes en el sentido de que se eliminarán los datos del cliente en ciertas ocasiones. Al cliente le puede interesar, no obstante, que el proveedor esté obligado a eliminar los datos, **metadatos** y sus copias de seguridad de forma inmediata, eficaz, irrevocable y permanente, siguiendo el calendario de conservación y eliminación de datos u otras formas de autorización o solicitudes comunicadas por el cliente al proveedor. El contrato puede abordar el plazo y otras condiciones para la eliminación de datos, como la obligación del proveedor de confirmar al cliente que los ha eliminado una vez que lo ha hecho y la de facilitarle el acceso a los registros de auditoría de las actividades de eliminación de datos.

81. Pueden especificarse determinadas normas o técnicas de eliminación de datos que han de aplicarse en función de la naturaleza y la sensibilidad de estos (por ejemplo, puede exigirse la eliminación de datos en distintos lugares y medios, como podría ser en los sistemas de los subcontratistas y otros terceros, en diferentes niveles, y llevarse a cabo desde un saneamiento de los datos que asegure su confidencialidad hasta su completa eliminación o la destrucción del equipo físico). Existen otros procedimientos de eliminación más seguros que conllevan la destrucción en lugar de la redistribución del equipo, pero pueden resultar más costosos y no siempre es posible llevarlos a cabo (si, por ejemplo, los datos de otros clientes del proveedor se almacenan en el mismo equipo). Es necesario tener en cuenta estos aspectos en la negociación del contrato, lo que podría lograrse exigiendo al proveedor que utilice una infraestructura aislada para almacenar los datos especialmente sensibles.

E. Auditorías y supervisión

- *Actividades de supervisión*

82. Es posible que las partes necesiten supervisar mutuamente sus actividades para garantizar el cumplimiento del contrato y de la normativa de regulación (por ejemplo, el cumplimiento por parte del cliente y sus usuarios finales de las **AUP** y **licencias de propiedad intelectual** y el cumplimiento por parte del proveedor del **SLA**, la política de protección de los datos, etc.). Algunas actividades de supervisión, como las relacionadas con el **procesamiento de datos personales**, pueden resultar obligatorias por ley.

83. El contrato debería establecer actividades de supervisión periódicas o recurrentes y determinar qué parte será responsable por su ejecución, así como establecer las obligaciones que debería cumplir la otra parte a fin de facilitar la supervisión. También se pueden prever en el contrato actividades excepcionales de supervisión, ofreciendo opciones para su gestión, así como los requisitos de notificación a la otra parte y los compromisos de confidencialidad relacionados con las actividades de supervisión.

84. Una supervisión excesiva puede afectar al desempeño y aumentar los costos de los servicios. En el caso de los servicios que deben prestarse casi en tiempo real, al cliente podría interesarle ejercitar el derecho a pedir al proveedor que interrumpa o ponga fin a la supervisión si ello supone un perjuicio importante para el funcionamiento de los servicios.

- *Auditorías y pruebas de seguridad*

85. Las auditorías y las pruebas de seguridad son bastante comunes, en especial las que inicia el proveedor para comprobar la eficacia de las medidas de seguridad. Algunas auditorías y pruebas de seguridad pueden ser obligatorias por disposición de la ley. El contrato puede incluir cláusulas que aborden los derechos de ambas partes en relación con la auditoría, su ámbito de aplicación, su frecuencia, sus formalidades y sus costos. También puede obligar a que las partes compartan entre sí los resultados de las auditorías o las pruebas de seguridad encargadas por cada una de ellas. Es posible que tanto los derechos contractuales como las obligaciones legales relacionadas con la auditoría y las pruebas de seguridad deban complementarse en el contrato con las obligaciones de la otra parte de facilitar el ejercicio de esos derechos o el cumplimiento de esas obligaciones (permitiendo, por ejemplo, el acceso a los centros de datos).

86. Las partes podrán pactar que las auditorías o las pruebas de seguridad solo puedan ser realizadas por organizaciones profesionales, o que el proveedor o el cliente puedan optar por que esas auditorías o pruebas sean llevadas a cabo por una organización profesional. En el contrato se pueden especificar los requisitos que deben cumplir dichos terceros y las condiciones para su participación, así como la distribución de los costos. Las partes pueden pactar acuerdos especiales para las auditorías o las pruebas de seguridad que deban realizarse tras producirse un incidente en función de la gravedad y naturaleza de este (por ejemplo, la parte responsable del incidente puede verse obligada a reembolsar total o parcialmente los gastos realizados).

F. Condiciones de pago

- *Pago por uso*

87. El precio es un elemento esencial del contrato. El hecho de no fijarse un precio o un mecanismo para su determinación puede hacer que no pueda exigirse el cumplimiento del contrato.

88. Una característica de los servicios de computación en la nube es la de ser **autoservicio a pedido**, por lo que el sistema de facturación suele ser del tipo "**pago por uso**" (*pay-as-you-go*). Es habitual que el contrato especifique el precio unitario de todos los servicios de computación en la nube acordados (por ejemplo, precio por número de usuarios, por número de usos o por tiempo de utilización). Las escalas de precios o los precios especiales, como los descuentos por volumen, pueden constituir incentivos o penalizaciones para cualquiera de las partes. Ofrecer servicios gratuitamente por un tiempo o no cobrar por algunos servicios es algo habitual. Aunque puede haber muchas variaciones en el cálculo de los precios, incluir una cláusula de precios clara y transparente que ambas partes entiendan puede evitar futuros conflictos y pleitos.

- *Derechos de licencia*

89. El contrato debería establecer claramente si el pago de los servicios de computación en la nube incluye los derechos de licencia correspondientes a las licencias que el proveedor pueda conceder al cliente como parte de los servicios. Los servicios **SaaS**, en especial, suelen conllevar la utilización por parte del cliente de programas informáticos con licencia del proveedor.

90. Los derechos de licencia pueden calcularse por usuario o por instancia y su importe puede variar en función de la categoría de usuarios (por ejemplo, los usuarios profesionales pueden ser una de las categorías más caras, frente a los no profesionales). El cliente debería valorar las implicaciones de las diversas formas de pago. Por ejemplo, el costo de licencia para un cliente puede aumentar de manera exponencial si los programas informáticos se cobran por instancia cada vez que se conecta una computadora nueva, aun cuando el cliente esté utilizando el mismo número de instancias para el mismo período. También puede resultar importante para el cliente determinar en el contrato, no solo el número de posibles usuarios de un programa informático que estarán amparados por el acuerdo de licencia, sino también el número de usuarios de

cada categoría (empleados, contratistas independientes, proveedores, etc.) y los derechos que se concederán a cada una de ellas. Además, el cliente puede querer que se recojan en el contrato los derechos de acceso y uso que estarán incluidos en la licencia, así como los casos de acceso y uso por parte del cliente y sus usuarios finales que pueden dar lugar a una ampliación del ámbito de aplicación de la licencia y, por consiguiente, a un aumento de los derechos que deben pagarse por usarla.

- *Costos adicionales*

91. El precio puede abarcar también los gastos puntuales (por ejemplo, la configuración y la migración a la nube). Pueden existir otros servicios adicionales no incluidos en el contrato básico de servicios de computación en la nube que el proveedor ofrezca a cambio de un pago aparte (por ejemplo, atención al cliente más allá del horario comercial facturando ese servicio por tiempo o asignándole un precio fijo). Las partes también deberían aclarar los efectos fiscales del contrato, ya que los servicios de computación en la nube pueden entrar o no dentro de la categoría de servicios o bienes imponibles.

- *Cambios en los precios*

92. Las condiciones estándar de los proveedores suelen conceder a estos el derecho a modificar unilateralmente el precio o las escalas de precios. No obstante, el cliente tal vez prefiera limitar ese derecho. Las partes pueden pactar la metodología de fijación de precios aplicable a su contrato (por ejemplo, con qué frecuencia y en qué medida el proveedor puede aumentar los precios). El aumento de los precios puede limitarse referenciando los precios a un índice de precios de consumo, utilizando un porcentaje fijo o empleando el listado de precios del proveedor en un momento dado. El cliente puede exigir al proveedor que este le notifique con antelación el aumento de precios y pueden fijarse en el contrato las consecuencias que tendría que el cliente no aceptara ese aumento.

- *Otras condiciones de pago*

93. Tal vez sea necesario incluir en las condiciones de pago una referencia a las modalidades de facturación (como la facturación electrónica) y a la forma y el contenido de las facturas, ya que puede resultar relevante a efectos de cumplir las normas tributarias. Es posible que las autoridades tributarias de algunas jurisdicciones no acepten facturas electrónicas o exijan un formato especial de factura, o puede ser que los impuestos aplicables a los servicios de computación en la nube deban detallarse por separado.

94. El contrato también debería especificar la fecha de pago, la moneda, el tipo de cambio aplicable, la forma de realizar el pago, las sanciones en caso de retrasos en los pagos y los procedimientos para resolver las controversias relativas a reclamaciones de pago.

G. Cambios en los servicios

95. Por naturaleza, los **servicios de computación en la nube** son flexibles y fluctuantes. El contrato puede incluir múltiples opciones que permitan al cliente adaptar los servicios a las necesidades cambiantes de su negocio. Además, el proveedor puede reservarse el derecho a modificar su cartera de servicios a su entera discreción. El régimen contractual apropiado en cada caso puede ser diferente en función de si los cambios se refieren a los principales servicios que se presten o a los servicios auxiliares y a cuestiones de asistencia. También podría estar justificado aplicar diferentes regímenes a los cambios que puedan afectar negativamente a los servicios y a aquellos que puedan suponer mejoras (por ejemplo, el paso de una oferta estándar de servicios de computación en la nube a una oferta mejorada con mayores niveles de seguridad o menores tiempos de respuesta).

- *Actualizaciones*

96. Si bien la aplicación de actualizaciones puede ser en interés del cliente, también puede causar trastornos en la disponibilidad de los servicios de computación en la nube, ya que podría conllevar períodos de **interrupción o corte del servicio** relativamente prolongados durante las horas normales de trabajo, aun cuando se trate de un servicio prestado ininterrumpidamente. También puede tener otros efectos negativos, como el tener que realizarse cambios en las aplicaciones del cliente o en sus sistemas informáticos,
o requerirse una nueva formación para los usuarios del cliente.

97. El contrato puede establecer la obligación del proveedor de notificar al cliente con suficiente antelación las actualizaciones que todavía falte aplicar y sus consecuencias. Se puede obligar al proveedor a que programe las actualizaciones durante los períodos en que la actividad del cliente sea escasa o nula. Cuando se vayan a realizar cambios significativos en la versión anterior las partes pueden acordar que se mantenga dicha versión en paralelo con la nueva durante un plazo convenido, a fin de garantizar la continuidad de las operaciones de los clientes. También puede ser necesario pactar los procedimientos que deben emplearse para comunicar y resolver posibles problemas. En el contrato tal vez sea necesario abordar también la cuestión de la asistencia que deberá prestar el proveedor cuando se realicen los cambios en las aplicaciones o los sistemas de tecnología de la información del cliente, así como la nueva formación que pudieran necesitar los usuarios finales del cliente. Es posible que las partes también necesiten pactar el reparto de los costos derivados de las actualizaciones.

- *Degradación o interrupción de los servicios*

98. Los avances tecnológicos, la presión de la competencia y otras circunstancias pueden llegar a provocar una degradación de algunos servicios de computación en la nube o su interrupción, y esos servicios pueden ser sustituidos o no por otros servicios. El proveedor puede reservarse en el contrato el derecho a modificar su oferta de servicios, por ejemplo, dando por finalizada una parte de estos. La interrupción de algunos servicios de computación en la nube por parte del proveedor puede obligar al cliente a asumir ciertas responsabilidades frente a sus usuarios finales.

99. En tales casos, el contrato tendría que disponer una protección adecuada para el cliente, como la obligación de enviar al cliente una notificación previa de los cambios, el derecho de este último a resolver el contrato si los cambios fueran inaceptables y un período de retención adecuado para garantizar la oportuna **reversibilidad** de los datos u otros contenidos afectados. El contrato puede prohibir totalmente las modificaciones que podrían afectar de forma negativa a la naturaleza, el alcance o la calidad de los servicios prestados, o bien limitar el derecho del proveedor a introducir únicamente “modificaciones razonables desde el punto de vista comercial”. No obstante, es posible que el cliente no esté en la mejor posición para juzgar la razonabilidad de las modificaciones de los servicios prestados y tal vez necesite el asesoramiento de expertos independientes.

- *Suspensión de servicios a discreción del proveedor*

100. Las condiciones estándar de los proveedores pueden contemplar su derecho a suspender los servicios a su entera discreción en cualquier momento. Al cliente podría interesarle limitar ese derecho incondicional y no permitir la suspensión, salvo en casos muy limitados (por ejemplo, en el caso de que se produzca un incumplimiento esencial del contrato por parte del cliente, como la falta de pago). La expresión “acontecimientos imprevisibles” se usa como una justificación habitual de la suspensión unilateral de los servicios por parte del proveedor. Dichos acontecimientos suelen definirse de una manera muy amplia para incluir cualquier obstáculo que esté más allá del control del proveedor, como los incumplimientos de sus subcontratistas, proveedores y otros terceros que participan en la prestación de los servicios de computación en la nube a los clientes, tales como los proveedores de acceso a Internet.

101. El cliente debe ponderar la posibilidad de condicionar el derecho del proveedor a suspender el servicio por acontecimientos imprevisibles a que este implante un plan de recuperación en casos de desastre y continuidad de las operaciones. El contrato puede disponer que este plan incluya medidas de protección frente a las amenazas más comunes para la prestación de los servicios de computación en la nube y que le sea enviado al cliente para su consideración y aprobación. Entre estas medidas de protección pueden figurar la existencia de un sitio de recuperación en casos de desastre geográficamente independiente al que pueda pasarse sin problemas en caso de desastre y la utilización de fuentes de alimentación ininterrumpida y generadores de apoyo.

- *Notificación de los cambios*

102. Las condiciones estándar de los proveedores pueden establecer que el proveedor no está obligado a notificar al cliente los cambios en las condiciones de los servicios. Es posible que se pida a los clientes que comprueben regularmente si se han producido cambios en los documentos contractuales alojados en el sitio o los sitios web del proveedor. Esos documentos contractuales pueden ser muy numerosos. Algunos pueden establecer condiciones y políticas que figuran en otros documentos haciendo referencia a ellos, y esos otros documentos pueden remitir a su vez a otras condiciones y políticas que pueden, todas ellas, ser objeto de modificación unilateral por parte del proveedor. Por lo tanto, podría resultar complicado que el cliente advierta los cambios introducidos por el proveedor.

103. Dado que la utilización continuada de los servicios por parte del cliente se considera como una aceptación de la modificación de las condiciones, al cliente podría interesarle que en el contrato se estableciera la obligación del proveedor de informarle sobre los cambios que se realicen en las condiciones de los servicios con suficiente antelación antes de su fecha de entrada en vigor. El contrato también puede establecer la obligación del proveedor de dar acceso al cliente a los registros de auditoría relativos a la evolución de los servicios. El cliente también podría estar interesado en mantener todas las condiciones pactadas y obligar al proveedor a que defina los servicios por referencia a una determinada versión.

H. Subcontratistas, proveedores del proveedor y externalización

- *Indicación de quienes intervengan en la cadena de subcontratación*

104. La subcontratación, los **servicios estratificados de computación en la nube** y la externalización son comunes en el campo de la **computación en la nube**. Las condiciones estándar de los proveedores pueden reservarle expresamente al proveedor el derecho a recurrir a terceros para prestar al cliente los servicios de computación en la nube, o este derecho puede resultar implícito debido a la propia naturaleza de los servicios que han de prestarse. Al proveedor le interesa conservar la mayor flexibilidad posible en ese sentido.

105. Sin embargo, la ley puede exigir que se indique en el contrato a los terceros que participan en la prestación de los servicios de computación en la nube al cliente; por otra parte, señalar a esos terceros puede ser positivo para el cliente al permitirle verificar información. Al cliente le podría interesar sobre todo obtener garantías relativas al cumplimiento por parte de terceros de los requisitos de seguridad, confidencialidad, protección de datos y otros similares derivados de lo previsto en el contrato o en la ley, la ausencia de conflictos de intereses y el riesgo de incumplimiento del contrato por el proveedor debido a los incumplimientos de terceros. Si bien el proveedor quizás no siempre pueda señalar a todos los terceros que participan en la prestación de los servicios de computación en la nube al cliente, debería poder indicar quiénes son los que desempeñan papeles fundamentales.

- *Cambios en la cadena de subcontratación*

106. El contrato puede prohibir que se realicen nuevos cambios en la cadena de subcontratación sin el consentimiento del cliente. Puede contemplarse el derecho del cliente a investigar los antecedentes de cualquier tercero que el proveedor quiera hacer participar en la prestación de sus servicios de computación en la nube y vetarlo. Como alternativa a lo anterior, puede incluirse en el contrato una lista de terceros previamente aprobados por el cliente y de entre los cuales el proveedor podrá elegir cuando surja la necesidad.

107. Sin embargo, el proveedor puede insistir en su derecho de hacer cambios unilaterales en su cadena de subcontratación, notificando o no al cliente esa circunstancia. El cliente puede reservarse el derecho a permitir que el proveedor realice el cambio, sujeto a su aprobación posterior. A falta de aprobación, se podría pactar que los servicios continuaran prestándose con el anterior tercero, con otros terceros previamente aprobados o con algún otro que las partes acuerden; de lo contrario, el contrato podría resolverse. La ley aplicable puede establecer en qué circunstancias los cambios en la cadena de subcontratación del proveedor pueden dar lugar a la resolución o rescisión del contrato.

- *Armonización de las condiciones contractuales con otros contratos vinculados*

108. Si bien es posible incluir en el propio contrato de computación en la nube un listado de los terceros que sean imprescindibles para cumplir el contrato, estos no serían partes en el contrato firmado entre el proveedor y el cliente. Ellos solo responderían de las obligaciones asumidas en virtud de su contrato con el proveedor. No obstante, pueden existir diversos mecanismos para garantizar que las condiciones del contrato suscrito entre el cliente y el proveedor resultan vinculantes para los terceros. En concreto, puede exigirse al proveedor que armonice las condiciones del contrato con las de otros contratos vigentes o futuros vinculados al primero. En el contrato también puede establecerse la exigencia de que el proveedor entregue al cliente copias de los contratos vinculados a los efectos de su comprobación.

109. El cliente puede optar por contratar directamente con los terceros que resultan imprescindibles para la ejecución del contrato de computación en la nube, en especial en cuestiones tan delicadas como la confidencialidad y el **procesamiento de datos personales**. También puede estar interesado en negociar con los terceros clave su obligación de intervenir en caso de que el proveedor no cumpla lo previsto en el contrato, como en caso de insolvencia del proveedor.

- *Responsabilidad de los subcontratistas, proveedores del proveedor y otros terceros*

110. Con arreglo a lo previsto en la legislación vigente o en el contrato, el proveedor puede ser considerado responsable frente al cliente por cualquier cuestión a cargo de un tercero que el proveedor haya contratado para la ejecución del contrato. En concreto, la ley puede establecer la responsabilidad conjunta del proveedor y sus subcontratistas en lo que respecta a las cuestiones que pudieran plantearse en materia de **procesamiento de datos personales**, según el grado de participación de los subcontratistas en el procesamiento.

111. En el contrato podría obligarse al proveedor a constituir derechos de terceros beneficiarios en los contratos vinculados en beneficio del cliente, o a hacer que el cliente fuera parte en dichos contratos vinculados. Ambas opciones permitirían que el cliente tuviera recurso directo contra el tercero en caso de que este último incumpliera el contrato vinculado.

I. Responsabilidad

- *Asignación de riesgos y responsabilidades*

112. En las transacciones entre empresas las partes disponen de libertad para distribuir los riesgos y las responsabilidades en la forma que estimen adecuada, cumpliendo siempre las disposiciones imperativas de la ley aplicable. En el momento de negociar la

distribución de los riesgos y las responsabilidades deberían tenerse en cuenta algunos factores como los riesgos asociados a la prestación de los servicios de computación en la nube, si dichos servicios se prestan a cambio de una remuneración o de alguna otra contraprestación, y el importe cobrado por el proveedor por tales servicios. Aunque las partes tienden a excluir o limitar la responsabilidad derivada de aquellos factores que no pueden controlar o que únicamente pueden controlar de forma limitada (como el comportamiento de los usuarios finales, las acciones u omisiones de los subcontratistas), el grado de control no será siempre un elemento decisivo. Las partes pueden estar dispuestas a asumir riesgos y responsabilidades por elementos que no pueden controlar como una forma de destacar en el mercado. Sin embargo, es más probable que los riesgos y responsabilidades de las partes aumenten progresivamente en función de los elementos que estén bajo su control.

113. Por ejemplo, en los servicios **SaaS** que conllevan la utilización de programas informáticos de oficina estándar, es probable que el proveedor deba responder de prácticamente todos los recursos proporcionados al cliente, haciéndose responsable en todos los casos en los que tales recursos no estén disponibles o no funcionen correctamente. No obstante, incluso en estos casos, el cliente podría tener que responder de todos modos de algunos componentes de los servicios, como el cifrado o las copias de seguridad de los datos bajo su control. El no haber realizado las copias de seguridad necesarias podría dar lugar a la pérdida del derecho a reclamar al proveedor en el caso de pérdida de los datos. Por otro lado, en el caso de servicios **IaaS** y **PaaS**, el proveedor únicamente tendría que responder de la infraestructura o las plataformas prestadas (como los equipos físicos, los sistemas operativos o los programas intermedios), mientras que el cliente respondería de todos los componentes que le pertenecieran, como las aplicaciones utilizadas en la infraestructura o las plataformas del proveedor y los datos alojados en ellas.

- *Exclusión o limitación de responsabilidad*

114. Las condiciones estándar de los proveedores pueden excluir toda responsabilidad contractual y señalar que las cláusulas de responsabilidad son innegociables. Por otra parte, también es posible que el proveedor esté dispuesto a aceptar su responsabilidad, incluso una responsabilidad ilimitada, por aquellas infracciones que estén bajo su control (por ejemplo, una violación de licencias de propiedad intelectual concedidas al proveedor por parte del cliente), pero no por aquellas otras derivadas de hechos que escapen a su control (como los incidentes de seguridad, los acontecimientos imprevisibles o las filtraciones de información confidencial). Las condiciones estándar de los proveedores suelen excluir su responsabilidad en caso de producirse daños indirectos o derivados (por ejemplo, la pérdida de oportunidades comerciales a raíz de la falta de disponibilidad de los servicios de computación en la nube).

115. Tanto en los casos en los que se acepta asumir responsabilidad de una forma general como en los que se acepta asumir responsabilidad en determinados casos, las condiciones estándar de los proveedores suelen limitar la cuantía de las pérdidas cubiertas (por siniestro, por serie de siniestros relacionados entre sí o por períodos de tiempo). Además, los proveedores suelen fijar un límite general de responsabilidad contractual que puede estar vinculado a los ingresos que se espera obtener del contrato, a la facturación del proveedor o a la cobertura del seguro.

116. Al cliente le puede interesar, no obstante, negociar una responsabilidad ilimitada o una indemnización mayor en caso de que se produzcan determinados tipos de daños por acciones u omisiones del proveedor o de su personal. La posibilidad de hacerlo puede depender, entre otros factores, del **modelo de despliegue** [*cross-link*]. Infracciones como la pérdida o el uso indebido de los datos de los clientes, las violaciones de las políticas de protección de datos personales y, en especial, la conculcación de los derechos de propiedad intelectual pueden dar lugar a una responsabilidad del cliente frente a terceros que quizás sea elevada o dar lugar a la imposición de multas reglamentarias. Puede estar justificado imponer al proveedor un régimen de responsabilidad más estricto cuando estas infracciones sean imputables a la culpa o a la negligencia de este. En el caso de algunos defectos (por ejemplo, defectos

en los equipos físicos o los programas informáticos), la ley puede establecer la responsabilidad ilimitada del proveedor.

117. Las condiciones estándar de los proveedores suelen hacer al cliente responsable por el incumplimiento de la **AUP**. Al cliente le puede interesar limitar su responsabilidad por el incumplimiento de la **AUP**, en especial cuando este incumplimiento tenga su origen en acciones de sus usuarios finales que el cliente no puede controlar.

118. Los descargos y las limitaciones de responsabilidad deberían figurar en el cuerpo principal del contrato y comunicarse adecuadamente a la otra parte para que fueran exigibles.

- *Seguro de responsabilidad civil*

119. En el contrato se pueden fijar determinadas obligaciones en materia de seguros para una o ambas partes, especialmente en lo que respecta a la calidad de la compañía de seguros y a la cuantía mínima de la cobertura contratada. También se puede exigir a las partes que notifiquen los cambios que se realicen en lo que respecta a la cobertura del seguro o que proporcionen a la otra una copia de las pólizas de seguro suscritas.

- *Requisitos legales*

120. Si bien la mayoría de los ordenamientos jurídicos reconocen el derecho de las partes contratantes a asignar los riesgos y las responsabilidades y a limitar o excluir su responsabilidad mediante disposiciones del contrato, este derecho suele estar sujeto a ciertos límites y condiciones. Por ejemplo, en lo que respecta al **procesamiento de datos personales**, un factor importante en la asignación de riesgos y responsabilidades es la función que cada parte asume en relación con los **datos personales** alojados en la nube. La legislación sobre protección de datos de muchas jurisdicciones impone una responsabilidad mayor al **responsable de los datos** que al **procesador de los datos personales**. A pesar de las disposiciones incluidas en el contrato, el manejo efectivo de esos datos será lo que normalmente determine el régimen jurídico al que estará sometida la parte en cuestión en virtud de lo previsto en la legislación aplicable. Los **sujetos de los datos** que hayan sufrido pérdidas resultantes de un procesamiento ilícito de **datos personales** o de cualquier actuación incompatible con las normas nacionales de protección de datos, pueden tener derecho a reclamar una indemnización directamente al **responsable de los datos**.

121. Además, muchas jurisdicciones no admiten o limitan las cláusulas que excluyen totalmente la responsabilidad derivada de la propia culpa. Tal vez no sea posible excluir en su conjunto la responsabilidad por lesiones (incluidas la enfermedad y el fallecimiento) o por negligencia grave, dolo, defectos, incumplimiento de las obligaciones básicas y esenciales para la ejecución del contrato o incumplimiento de los requisitos reglamentarios aplicables. Además, si los términos del contrato no se han negociado libremente, sino que han sido impuestos o vienen preestablecidos por una de las partes (“contratos de adhesión”), algunos tipos de cláusulas de limitación de responsabilidad pueden considerarse “abusivas” y, por tanto, nulas [*cross-link*].

122. Las instituciones públicas pueden ver limitada por ley su capacidad para asumir determinadas responsabilidades, o pueden necesitar la autorización previa de un órgano estatal competente para poder hacerlo. También pueden tener prohibido aceptar cláusulas que limiten o excluyan la responsabilidad de un proveedor en su totalidad o por las acciones u omisiones definidas en la legislación.

123. Por otra parte, la ley aplicable puede establecer la eximente de responsabilidad de una de las partes si cumple ciertos criterios que, de no satisfacerse, podrían hacer incurrir a esa parte en responsabilidad. Por ejemplo, según el procedimiento de “detección y retirada” vigente en algunas jurisdicciones, el proveedor quedará liberado de responsabilidad por alojar contenido ilegal en su infraestructura de nube si retira dicho contenido una vez tenga conocimiento de su ilegalidad [*cross-link*].

J. Recursos disponibles en caso de incumplimiento de contrato

- *Tipos de recursos disponibles*

124. Dentro de los límites previstos por la ley aplicable, las partes están facultadas para elegir libremente los recursos jurídicos que desean emplear. Entre ellos cabe mencionar las acciones orientadas a obtener una reparación en especie destinada a proporcionar a la parte perjudicada un beneficio idéntico o equivalente al que se esperaba obtener del cumplimiento del contrato (por ejemplo, la sustitución del equipo físico defectuoso), compensaciones pecuniarias (por ejemplo, créditos para la utilización de servicios) y la posibilidad de resolver el contrato. El contrato podría contemplar diferentes tipos de incumplimientos y especificar las medidas que se podrían adoptar en cada caso.

- *Suspensión o cancelación de los servicios*

125. Suspender o cancelar la prestación al cliente de los servicios de computación en la nube es una medida habitual que puede adoptar el proveedor ante un incumplimiento del contrato por parte del cliente, o ante una transgresión de la **AUP** por parte de los usuarios finales del cliente. Al cliente le podría interesar disponer de ciertas salvaguardas que lo protegieran del ejercicio de un derecho muy amplio de suspensión o cancelación de los servicios por parte del proveedor. Por ejemplo, puede limitarse el derecho del proveedor a suspender o cancelar los servicios de computación en la nube al cliente a los casos en que el proveedor incurra en un incumplimiento esencial del contrato y de que se presenten amenazas importantes para la seguridad o la integridad del sistema del proveedor. El derecho del proveedor a suspender o cancelar el servicio también podría restringirse únicamente a los servicios afectados por el incumplimiento, cuando exista esta posibilidad.

- *Créditos para la utilización de servicios*

126. Un mecanismo que suele utilizarse para compensar al cliente por el incumplimiento del proveedor es el sistema de créditos para la utilización de servicios. Estos créditos consisten en el ofrecimiento de una reducción en el precio de los servicios contratados que se prestarán en el siguiente período de servicio. Se puede aplicar una escala variable, es decir, el porcentaje que se descuente puede depender de la medida en que el servicio prestado por el proveedor no satisfaga los parámetros de desempeño establecidos en el **SLA** o en otras partes del contrato. También se puede aplicar un límite general a los créditos para la utilización de servicios. Los proveedores pueden limitar los créditos a aquellos casos en los que, por ejemplo, los fallos se deban a cuestiones que estén bajo el control del proveedor o disponer que dichos créditos se utilicen dentro de un plazo determinado. Algunos proveedores también pueden estar dispuestos a reembolsar las sumas pagadas u ofrecer un paquete de servicios mejorado durante el período del servicio siguiente (ofreciendo, por ejemplo, consultoría gratuita sobre tecnología de la información). En los casos en que existen varias opciones disponibles, las condiciones estándar de los proveedores suelen establecer que serán ellos mismos quienes elegirán la forma de compensar por su incumplimiento.

127. El cliente debería evaluar en cada caso si el hecho de que se establezca en el contrato que se otorgarán créditos para la utilización de servicios como única medida para compensar el incumplimiento por parte del proveedor de sus obligaciones contractuales resulta lo más idóneo. Pactar créditos para la utilización de servicios como única forma de reparación puede limitar el derecho del cliente a solicitar otras medidas de resarcimiento, como interponer una demanda por daños y perjuicios o resolver el contrato. Al cliente le puede interesar que el contrato prevea otras medidas para mitigar los riesgos de incumplimiento del proveedor y establezca incentivos suficientes para que el proveedor cumpla adecuadamente sus obligaciones contractuales y mejore los servicios. Las penalizaciones, por ejemplo, podrían tener un efecto económico mayor sobre el proveedor que los créditos para la utilización de servicios. Además, ofrecer créditos que consistan en una reducción del precio o un paquete mejorado en el período de servicio siguiente puede resultar inútil si el contrato está a punto de extinguirse. Puede resultar imposible gastar una cantidad excesiva de créditos si al comienzo del

contrato se cometió el error de considerar que esos créditos alcanzarían para compensar de forma aproximada el daño causado.

- *Formalidades que han de seguirse en caso de incumplimiento del contrato*

128. En el contrato pueden preverse las formalidades que deben seguirse en los casos de incumplimiento contractual. Por ejemplo, se podría establecer que la parte que considera que se ha producido algún incumplimiento notifique a la otra esta supuesta circunstancia, ofreciéndole la oportunidad de subsanar ese incumplimiento. También es posible fijar ciertos plazos para solicitar las medidas de reparación.

K. Duración y extinción del contrato

- *Fecha efectiva de entrada en vigor del contrato*

129. En el contrato debería establecerse de forma clara su fecha efectiva de entrada en vigor. Esta puede ser diferente de la fecha de firma, de la fecha de aceptación de la oferta o de la fecha de aceptación de la configuración y demás acciones necesarias para que el cliente migre sus contenidos a la nube. Puede considerarse como la fecha efectiva de entrada en vigor del contrato aquella en la que el proveedor pone a disposición del cliente los servicios de computación en la nube, aunque el cliente no los utilice efectivamente en ese momento. También puede considerarse como fecha efectiva de entrada en vigor aquella en la que el cliente realice el primer pago por los servicios de computación en la nube, incluso aunque en ese momento el proveedor no los haya puesto todavía a disposición del cliente.

- *Duración del contrato*

130. La duración del contrato puede ser corta, media o larga. En el caso de las **soluciones de nube genéricas y estandarizadas para múltiples suscriptores** es habitual establecer una duración inicial determinada (corta o media) con prórrogas automáticas, salvo que el contrato sea resuelto por alguna de las partes. El cliente puede exigir que el proveedor le notifique el próximo vencimiento del plazo del contrato y la necesidad de que el cliente tome una decisión sobre su renovación. Este mecanismo puede ser útil para el cliente a los efectos de evitar el riesgo de **dependencia de la solución tecnológica** y poder conseguir mejores condiciones.

- *Rescisión y resolución del contrato*

131. En el contrato pueden recogerse las circunstancias en las cuales puede darse por extinguido por causas distintas al vencimiento del plazo fijado en él, es decir, por conveniencia de las partes, incumplimiento u otras razones. El contrato podría prever distintas modalidades de resolución anticipada, así como los requisitos que deben cumplirse para que la notificación se produzca con suficiente antelación, las cuestiones relacionadas con la **reversibilidad** y otras obligaciones relativas a la finalización del servicio [*cross-link*].

Resolución del contrato por razones de conveniencia

132. Las cláusulas estándar de los proveedores, especialmente las relativas a la prestación de **soluciones de nube genéricas y estandarizadas para múltiples suscriptores**, suelen reservar a los proveedores el derecho a resolver el contrato en cualquier momento, sin necesidad de que exista incumplimiento del cliente. Al cliente podría interesarle limitar las circunstancias en las que se pueda ejercitar este derecho y obligar a que el proveedor le notifique con suficiente antelación su voluntad de resolver el contrato.

133. El derecho del cliente a resolver el contrato por razones de conveniencia (es decir, sin que exista incumplimiento del proveedor) es especialmente frecuente en los contratos públicos. En tales casos, el proveedor puede exigir el pago de una indemnización por resolución anticipada. No obstante, esos pagos, cuando los hacen entidades públicas, pueden estar sujetos a restricciones legales. En los contratos de duración indefinida, los proveedores quizás prefieran aceptar que el cliente tenga derecho a resolver el contrato por razones de mera conveniencia sin derecho a una indemnización, pero ello podría conllevar también un precio más elevado en el contrato.

Resolución por incumplimiento

134. Un incumplimiento esencial del contrato justifica generalmente la resolución de este. Para evitar ambigüedades, las partes pueden establecer en el contrato los supuestos que han de considerarse un incumplimiento esencial. Para el cliente, esos supuestos pueden ser la pérdida o el uso indebido de los datos, las violaciones de la política de protección de datos personales, la recurrencia de los incidentes de seguridad (cuando se produzcan, por ejemplo, más de X veces en el período medido), las fugas de información confidencial y la indisponibilidad de los servicios en determinados momentos o durante un determinado período de tiempo. En el caso del proveedor, la falta de pago por parte del cliente y la violación por el cliente o sus usuarios finales de la **AUP** son algunos de los motivos más comunes que le facultan a resolver el contrato. El derecho de las partes a resolver el contrato puede estar sujeto al requisito de que se emita una notificación previa, de que se celebren consultas de buena fe, de que se ofrezca la posibilidad de subsanar el incumplimiento y de que no se haya asumido la obligación de reiniciar el cumplimiento del contrato en un determinado número de días tras la adopción de las medidas correctivas.

135. En el contrato se pueden establecer las obligaciones relacionadas con la finalización del servicio que hubiera asumido el proveedor y que subsistirían tras un incumplimiento esencial del cliente. Al cliente le puede interesar que se garantice, como mínimo, la **reversibilidad** de sus datos y otros contenidos [*cross-link*].

Rescisión por modificaciones inaceptables del contrato

136. Las modificaciones introducidas en el contrato que resulten inaceptables, que no sean razonables desde el punto de vista comercial o que sean unilaterales y produzcan un perjuicio grave pueden justificar la rescisión del contrato. Entre ellas podrían citarse las modificaciones de los requisitos relativos a la **ubicación de los datos** o las condiciones de subcontratación. Debería preservarse, en particular, el derecho del cliente a rescindir el contrato en su totalidad cuando las modificaciones introducidas en él a causa de una reestructuración de la cartera de servicios del proveedor tuvieran como resultado la cancelación o sustitución de algunos servicios [*cross-link*].

Rescisión en caso de insolvencia

137. Es posible que el cliente insolvente tenga la necesidad de seguir utilizando los servicios de computación en la nube mientras resuelve sus dificultades financieras. En esos casos, al cliente le puede interesar que se limite el derecho del proveedor a invocar su situación de insolvencia como único motivo para rescindir el contrato cuando no concurriera otro, por ejemplo, la falta de pago del cliente.

138. Es posible que durante la evaluación de los riesgos se contemple la posibilidad de que el proveedor se vuelva insolvente. En el contrato puede establecerse la obligación del proveedor de suministrar al cliente informes periódicos sobre su situación financiera y concederle el derecho a rescindir el contrato, sin ninguna obligación o responsabilidad para el cliente, en el caso de que el proveedor carezca de la capacidad financiera necesaria para cumplir cabalmente el contrato.

139. Cuando se retira una gran cantidad de contenidos como consecuencia de una crisis de confianza ocasionada por la situación financiera del proveedor, existe un riesgo elevado de que no se puedan recuperar nunca los datos y otros contenidos alojados en la infraestructura de nube de un proveedor insolvente. Tanto el proveedor insolvente

como el **representante de la insolvencia** pueden limitar la cantidad de contenido (datos y código de las aplicaciones) que pueden retirarse en un período determinado. También pueden decidir que las obligaciones relativas a la finalización del servicio se lleven a cabo por orden cronológico. Al cliente le podría interesar, por lo tanto, disponer de mecanismos contractuales que le aseguren que podrá recuperar sus datos del proveedor insolvente. El cliente podría solicitar que se liberen automáticamente el código fuente o las claves de custodia para tener acceso a sus datos y otros contenidos tras declararse la insolvencia del proveedor. No obstante, podrían existir disposiciones imperativas en el régimen de la insolvencia que dejaran sin efecto obligaciones establecidas en el contrato.

Resolución en caso de cambio de control

140. El cambio de control puede suponer, por ejemplo, un cambio en la titularidad o la capacidad para determinar, directa o indirectamente, las políticas operacionales y financieras del proveedor, lo que puede dar lugar a cambios en su cartera de servicios. El cambio del control también puede entrañar la cesión o la novación del contrato, transmitiéndose a un tercero los derechos y las obligaciones (o solo los derechos) previstos en el contrato. Como resultado de ello, podría cambiar alguna de las partes originales en el contrato o ciertos aspectos de este. Por ejemplo, es posible que los pagos deban realizarse a un tercero.

141. En el contrato puede establecerse la obligación del proveedor de notificar con antelación un próximo cambio de control, así como los efectos que se prevé tenga ese cambio en la continuidad de los servicios. Al cliente le puede interesar reservarse en el contrato el derecho a resolverlo si, como consecuencia del cambio de control, un competidor del cliente adquiere la empresa del proveedor o lo sucede como parte en el propio contrato o si el cambio de control conduce a la discontinuación de los servicios o a cambios significativos en los mismos. El derecho aplicable puede disponer que se dé por extinguido el contrato si, como consecuencia del cambio de control, no pudieran cumplirse los requisitos exigidos por ley (por ejemplo, los requisitos de ubicación de los datos o la prohibición de hacer negocios con determinadas entidades porque estuvieran sujetas a un régimen internacional de sanciones o por motivos de seguridad nacional). Los contratos públicos pueden verse especialmente afectados por restricciones legales relacionadas con cambios de control.

Cláusula sobre cuentas inactivas

142. La inactividad del cliente durante un determinado período de tiempo especificado en el contrato puede dar derecho al proveedor a resolverlo unilateralmente. No obstante, es bastante raro que se incluya una cláusula de cuentas inactivas en los contratos de computación en la nube entre empresas celebrados a título oneroso.

L. Obligaciones relativas a la finalización del servicio

143. Es posible que las obligaciones relativas a la finalización del servicio no solo den lugar a problemas contractuales, sino también regulatorios. En el contrato debería alcanzarse un equilibrio entre el interés del cliente en disponer de acceso continuo a sus datos y otros contenidos (incluso durante el período de transición) y el del proveedor en poner fin lo antes posible a toda obligación que pudiera tener con el antiguo cliente.

144. Las obligaciones relativas a la finalización del servicio pueden ser las mismas para cualquier causa de extinción del contrato, o pueden ser diferentes cuando el contrato se extingue por un incumplimiento o por otras razones. Entre las cuestiones que las partes deberían resolver en el contrato figuran las siguientes:

- *Plazo para la exportación*

145. Al cliente le podría interesar disponer de un plazo suficientemente prolongado para asegurarse de que la transferencia de sus datos y otros contenidos a otro proveedor o a sus propios sistemas se realizará sin tropiezos.

- *Acceso del cliente al contenido que se ha de exportar*

146. El contrato debería especificar los datos y otros contenidos que han de exportarse, así como la forma en que el cliente podrá acceder a ellos, incluidas las claves de descifrado que puedan estar en poder del proveedor o de terceros. Las partes pueden pactar un sistema de custodia que garantice el acceso automático del cliente a todos los atributos necesarios para la exportación. El contrato también puede especificar, en la medida de lo posible, las diferentes opciones que existen para la exportación, como sus formatos y procesos, y disponer que pueden cambiar con el tiempo.

- *Asistencia por parte del proveedor durante la exportación*

147. Podría especificarse en el contrato el período durante el cual el proveedor de servicios de nube intervendrá en la exportación de los datos del cliente a sus propios sistemas o a los de otro proveedor de su elección, así como el alcance de su intervención y el procedimiento que se ha de seguir El proveedor puede exigir un pago aparte por la prestación de asistencia durante la exportación. En ese caso, las partes pueden fijar en el contrato la cuantía de dicho pago o remitir en el contrato al listado de precios del proveedor vigente en un momento dado. Otra posibilidad consistiría en que las partes acordaran que esta asistencia estuviera incluida en el precio del contrato o que no se pudiera cobrar ninguna suma de dinero adicional si el contrato se extinguiera por incumplimiento del proveedor.

- *Eliminación de los datos de la infraestructura de nube del proveedor*

148. El contrato podría precisar normas para la eliminación de los datos y otros contenidos del cliente de la infraestructura de nube del proveedor para cuando hayan sido exportados o para cuando haya concluido el plazo especificado en el contrato para llevar a cabo la exportación. Los datos pueden ser eliminados automáticamente por el proveedor o previa solicitud del cliente siguiendo sus instrucciones. El contrato puede establecer que el proveedor avise al cliente antes de eliminar los datos y que confirme a este último que sus datos, copias de seguridad y **metadatos** han sido eliminados. El proveedor puede estar obligado a entregar un certificado, un informe o una declaración de eliminación de contenidos que incluya la información sobre la eliminación de los contenidos de sistemas de terceros.

- *Conservación de los datos con posterioridad a la extinción del contrato*

149. El proveedor puede estar obligado por ley, en especial por las leyes de protección de datos, a conservar los datos de los clientes, y la ley puede fijar también el plazo durante el cual deben mantenerse dichos datos. Además, el cliente puede autorizar al proveedor a conservar determinados datos o exigir que este se obligue por contrato a conservarlos una vez extinguido el contrato por distintas razones, por ejemplo, por razones de regulación, porque pueden requerirse en un proceso judicial o por otras razones legales que afecten al cliente. Algunos proveedores quizás acepten que el cliente determine el plazo durante el cual han de conservarse los datos tras la extinción del contrato, a cambio de un costo adicional.

150. Tal vez sea necesario establecer determinadas obligaciones relativas a los datos que no se devolverán o que no podrán ser devueltos al cliente y cuya eliminación no resulte posible (por ejemplo, la obligación de que se adopten medidas respecto de los datos personales que impidan la identificación). En el contrato se debería especificar el formato en que se conservarán esos datos una vez que el contrato se haya extinguido. El formato puede ser uno aprobado por el cliente (un formato cifrado o no cifrado), o el contrato puede disponer, de una forma general, que los datos se conservarán en un formato flexible y versátil que permita la recuperación en caso necesario. En el contrato se deberían establecer las obligaciones que tendrán las partes en relación con la conservación de los datos en el formato especificado una vez extinguido el contrato.

- *Cláusula de confidencialidad para después de la extinción del contrato*

151. Las partes pueden pactar una cláusula de confidencialidad para después de la extinción del contrato. Las obligaciones de confidencialidad pueden subsistir más allá de la vida del contrato, por ejemplo, durante un plazo de cinco a siete años después de operada su extinción o pueden prolongarse indefinidamente, en función de la naturaleza de los datos y otros contenidos del cliente alojados en la infraestructura de nube del proveedor.

- *Auditorías posteriores a la extinción del contrato*

152. Las auditorías posteriores a la extinción del contrato pueden ser acordadas por las partes o impuestas por la ley. El contrato debería contener disposiciones sobre la realización de esas auditorías, por ejemplo, su calendario y la distribución de sus costos.

- *Saldo remanente en cuenta*

153. Las partes pueden llegar a un acuerdo sobre las condiciones que deben darse para que se devuelvan al cliente las sumas remanentes en su cuenta, a fin de que estas puedan utilizarse como compensación de los pagos que el cliente tenga pendientes con el proveedor (en particular, por las actividades relativas a la finalización del servicio), o de que se imputen al pago de una indemnización por daños y perjuicios.

M. Solución de controversias

- *Mecanismos de solución de controversias*

154. Es aconsejable que las partes pacten el mecanismo que utilizarán para resolver las controversias que puedan surgir del contrato. Entre los mecanismos de solución de controversias posibles figuran la negociación, la mediación, la conciliación, el arbitraje y el proceso judicial. Diferentes tipos de controversias pueden justificar que se utilicen distintos procedimientos. Por ejemplo, las controversias sobre cuestiones financieras y técnicas quizás se sometan a la decisión vinculante de un perito independiente (que puede ser un individuo o un órgano), mientras que otro tipo de conflictos tal vez se resuelvan más eficazmente mediante negociaciones directas entre las partes. La legislación vigente en algunas jurisdicciones a veces obliga a las partes a recurrir a ciertos mecanismos alternativos de solución de controversias que las partes deben agotar antes de poder someter su controversia a la decisión de un tribunal nacional.

- *Proceso arbitral*

155. Las controversias que no se hayan resuelto de una forma amistosa pueden someterse a arbitraje, si las partes optaron por este mecanismo. Las partes deben verificar si las cuestiones en disputa pueden ser sometidas a arbitraje (es decir, deben comprobar si las cuestiones que desean someter a la decisión del árbitro solo pueden ser planteadas ante un tribunal de justicia según la ley del Estado). Si las partes optan por el arbitraje, es aconsejable que pacten las normas que deberán regir el proceso arbitral. El contrato puede incluir una cláusula estándar de solución de controversias que disponga la aplicación de normas reconocidas internacionalmente para llevar a cabo el proceso en cuestión (como el Reglamento de Arbitraje de la CNUDMI). A falta de una cláusula de ese tipo, el proceso arbitral se regirá normalmente por el derecho procesal del Estado en que tenga lugar o, si las partes eligen una institución arbitral, por las normas de dicha institución. Las partes pueden optar por un mecanismo de solución de controversias en línea que tenga su propio reglamento.

- *Proceso judicial*

156. En caso de iniciarse un proceso judicial podría suceder que, debido a la naturaleza de los **servicios de computación en la nube**, varios Estados consideren tener competencia sobre el litigio. En la medida de lo posible, es conveniente que las partes convengan en una cláusula en que establezcan que someterán sus controversias a un tribunal determinado [*cross-link*].

- *Conservación de datos*

157. El contrato debería abordar cuestiones relacionadas con la conservación de los datos y otros contenidos del cliente y su acceso a estos por parte del cliente durante un período de tiempo razonable, con independencia de la naturaleza de la controversia. Esto puede ser importante para el cliente, no solo por la necesidad de garantizar la continuidad de sus operaciones, sino también porque el acceso a los datos, incluidos los **metadatos** y otros **datos obtenidos de los servicios de nube**, puede resultar vital en el propio proceso de solución de controversias (por ejemplo, para fundamentar una demanda o una reconvención).

- *Plazo de prescripción para la presentación de reclamaciones*

158. Las partes pueden llegar a un acuerdo sobre los plazos en los que podrán presentarse las reclamaciones. Es posible que los proveedores quieran imponer a los clientes plazos relativamente breves para la presentación de reclamaciones relacionadas con los servicios. Las cláusulas que se estipulen al respecto pueden resultar inaplicables si los plazos establecidos en ellas no son los plazos de prescripción obligatorios previstos en la ley.

N. Cláusulas de elección de la ley y el foro

159. La libertad de contratación normalmente permite que las partes elijan la ley que se aplicará a su contrato y la jurisdicción o el foro en el que serán examinadas sus controversias. No obstante, y en función del objeto de la controversia, es posible que el derecho imperativo (por ejemplo, la legislación sobre protección de datos) prevalezca por sobre las cláusulas de elección de la ley y el foro pactadas por las partes contratantes. Además, independientemente de la ley y el foro que las partes elijan, es posible que resulte obligatoria la aplicación al contrato de más de un conjunto de disposiciones legales (por ejemplo, las leyes sobre protección de datos, régimen de la insolvencia, etc.).

- *Cuestiones que deben tenerse en cuenta a la hora de elegir la ley y el foro*

160. Las cláusulas de elección de la ley y el foro están relacionadas entre sí. El que pueda aplicarse la ley elegida y convenida depende, en última instancia, del foro ante el cual se invoque la cláusula de elección de la ley, sea que se trate de un tribunal de justicia u otro órgano decisor (como un tribunal arbitral). Será la ley de dicho foro la que determine si la cláusula es o no válida y si el foro respetará o no la elección de la ley hecha por las partes. Dada la importancia que tiene la ley del foro para la cláusula de elección de la ley, los contratos que contemplan esta cláusula también suelen incluir una cláusula de elección del foro.

161. Al elegir el foro, las partes suelen tener en cuenta los efectos de la ley elegida o aplicable y en qué medida se reconocerá y aplicará una resolución judicial de ese foro en los países en los que probablemente se solicite su ejecución. Podría resultar conveniente preservar la flexibilidad en relación con las opciones que existan para la ejecución, especialmente en los entornos de **computación en la nube** en los que puede resultar difícil determinar ciertos factores como la ubicación de los activos en relación con los cuales se prestan los servicios, el proveedor y el cliente, y otros factores que las partes suelen tener en cuenta al redactar las cláusulas de elección de la ley y el foro.

- *Derecho imperativo y foro*

162. La ley y el foro de una jurisdicción determinada pueden ser obligatorios por diversos motivos, a saber:

a) que la accesibilidad de los servicios de computación en la nube en el territorio de un Estado determinado pueda ser suficiente para aplicar sus leyes sobre protección de datos;

b) que la nacionalidad o la residencia del **sujeto de los datos** o de las partes contratantes, en especial del **responsable de los datos**, puedan dar lugar a la aplicación de la ley del **sujeto de los datos** o de alguna de las partes; y

c) que la ley del lugar en que se originó la actividad (la ubicación del equipo) o a la que se orienta la actividad con fines de lucro haga que se aplique la ley de ese lugar. La utilización de nombres de dominio geográficos asociados a un lugar determinado, el idioma local utilizado por el proveedor en sus páginas web, el hecho de que se hayan fijado los precios en una moneda local y la existencia de personas de contacto locales son algunos de los factores que podrían influir en esa determinación.

- *Ley y foro del proveedor o del cliente*

163. Los contratos de s**oluciones de nube genéricas y estandarizadas para múltiples suscriptores** suelen especificar que se rigen por el derecho de la sede principal de negocios del proveedor o su principal centro de actividades y suelen otorgar a los tribunales del país del proveedor competencia exclusiva sobre todas las controversias derivadas del contrato. El cliente tal vez prefiera que se establezca la ley y la jurisdicción de su propio país. Por lo general, pesan sobre las entidades públicas importantes restricciones para aceptar la ley de otro país y la competencia de tribunales extranjeros. Es posible que los proveedores que realizan sus actividades en numerosas jurisdicciones sean flexibles en lo que respecta a la elección de la ley y el foro del país en el que se encuentra el cliente.

- *Multiplicidad de opciones*

164. Las partes pueden también prever diversas opciones para distintos aspectos del contrato. Por ejemplo, pueden optar por la jurisdicción del demandado para que el demandante no cuente con la ventaja de poder accionar en su propio foro, fomentando así la solución informal de controversias.

- *Ausencia de cláusulas de elección de ley y foro*

165. Algunas partes pueden preferir no incluir cláusulas de elección de ley y foro en su contrato, dejando la cuestión abierta para ser tratada y resuelta más adelante, de ser necesario. En algunos casos, esta solución podría considerarse la única viable.

O. Notificaciones

166. Las cláusulas relativas a las notificaciones establecen la forma y el idioma de la notificación, así como quién debe recibirla, los medios de notificación que han de emplearse, y el momento en que la notificación se considera realizada (el momento de la entrega, del envío o del acuse de recibo). A falta de disposiciones legales de aplicación obligatoria, las partes pueden acordar las formalidades que pueden utilizar para efectuarlas, que pueden ser uniformes o variar según el grado de importancia de la notificación, su urgencia y otras consideraciones. Por ejemplo, en el caso de las notificaciones de suspensión o resolución unilateral del contrato pueden justificarse formalidades más estrictas que las aplicables a las notificaciones rutinarias. En tales casos, los plazos máximos previstos para la notificación deberían permitir la **reversibilidad** y la continuidad de las operaciones del cliente. El contrato puede contener referencias a las notificaciones y a los plazos impuestos por ley.

167. Las partes pueden decidir que las notificaciones se realicen **por escrito** y que se envíen a la dirección electrónica o se entreguen en la dirección física de las personas de contacto que figuran en el contrato. El contrato puede establecer los efectos jurídicos de no notificar o de no responder a una notificación a la que debe contestarse.

P. Otras cláusulas

168. A menudo las partes agrupan bajo el epígrafe “otras cláusulas” diversas cláusulas para las que no encuentran una ubicación más adecuada en otras partes del contrato. Algunas de ellas (denominadas “cláusulas tipo”) tienen una redacción estándar que suele usarse en todo tipo de contratos mercantiles, como la cláusula de divisibilidad que permite no tener en cuenta las disposiciones inválidas sin que ello afecte la validez del resto del contrato, o la cláusula en que se establece que la versión del contrato redactada en un determinado idioma es la que prevalecerá sobre las demás versiones en caso de que hubiera discrepancias respecto de su interpretación. El hecho de que estas cláusulas se incluyan en un apartado común junto con otras cláusulas varias no disminuye su importancia desde el punto de vista jurídico. Algunas de ellas quizás deban ser examinadas cuidadosamente por las partes teniendo en cuenta las distintas particularidades de la computación en la nube.

Q. Modificación del contrato

169. Cualquiera de las partes puede proponer modificaciones al contrato. En el contrato debería establecerse el procedimiento que ha de seguirse para que las modificaciones que se introduzcan sean eficaces. También pueden preverse las consecuencias que tendría el rechazo de las modificaciones por cualquiera de las partes.

170. Habida cuenta de la naturaleza de la **computación en la nube**, podría ser difícil determinar si un cambio que se hiciera supondría una modificación del contrato. Por ejemplo, la utilización por el cliente de las opciones disponibles en el contrato desde el principio no constituiría necesariamente una modificación del contrato inicial, como tampoco constituirían una modificación los cambios que se hicieran en los servicios que se prestaran como parte de operaciones rutinarias de mantenimiento y otras actividades del proveedor previstas en el contrato. Por el contrario, el hecho de añadir funcionalidades no previstas en las condiciones acordadas inicialmente y el cambio de precio que fuera consecuencia de esa adición pueden constituir una modificación del contrato. Las actualizaciones que produzcan cambios sustanciales en las condiciones y políticas acordadas previamente también pueden constituir una modificación del contrato. Las modificaciones sustanciales de las cláusulas esenciales del contrato firmado inicialmente (como la supresión de algunos servicios de computación en la nube) pueden dar lugar a un nuevo contrato.

171. La modificación de los contratos públicos puede verse limitada por las normas que rigen la contratación pública, que generalmente restringen la libertad de las partes para volver a negociar las cláusulas de un contrato sujetas a las disposiciones que rigen los procedimientos de licitación pública.

172. En caso de que se realizaran modificaciones frecuentes a las condiciones convenidas originalmente, cada una de las partes podría guardar separadamente de la otra la totalidad de las cláusulas acordadas inicialmente y sus modificaciones.

Glosario

Política de uso aceptable (**AUP, por sus siglas en inglés**): parte del contrato de computación en la nube celebrado entre el proveedor y el cliente que define los límites del uso por el cliente y sus usuarios finales de los servicios de computación en la nube previstos en el contrato estableciendo, por ejemplo, que el cliente y sus usuarios finales no podrán alojar ni utilizar contenidos ilegales o prohibidos en la nube [*cross-link*].

Auditoría: proceso consistente en examinar el cumplimiento de los requisitos legales y contractuales. Puede abarcar aspectos técnicos, como la calidad y la seguridad de los equipos físicos y los programas informáticos; el cumplimiento de la normativa aplicable al sector; y la existencia de medidas adecuadas, como el aislamiento, para impedir el acceso no autorizado al sistema y su uso, y para garantizar la integridad de los datos. Puede ser interna (realizada por el proveedor) o externa (realizada por el cliente o un tercero independiente, nombrado por el proveedor, por el cliente o por ambas partes).

Computación en la nube: suministro y utilización de los **servicios de computación en la nube** a través de redes abiertas o cerradas. Puede tener las siguientes características:

a) **acceso amplio a la red: posibilidad de acceder a los servicios de computación en la nube** a través de la red desde cualquier lugar en que la red esté disponible (por ejemplo, a través de Internet), utilizando muy diversos dispositivos, como teléfonos móviles, tabletas y computadoras portátiles;

b) **servicio medido**: suministro de **servicios de computación en la nube** sujetos a medición, como en el sector de los servicios públicos (gas, electricidad, etc.), que permite llevar un registro de los recursos utilizados y cobrarlos en función de su uso (conforme a un régimen de **pago por uso**);

c) **recursos compartidos**: asignación de recursos físicos y virtuales a múltiples usuarios cuyos datos se encuentran aislados, de manera que ninguno de ellos pueda acceder a los datos de los demás;

d) **autoservicio a pedido**: **servicios de computación en la nube** que son utilizados por el cliente cuando este los necesita, automáticamente o con una interacción mínima con el proveedor;

e) **elasticidad y escalabilidad**: capacidad de ampliar o reducir rápidamente el consumo de los **servicios de computación en la nube**, con arreglo a las necesidades del cliente, teniendo en cuenta las grandes tendencias en el uso de los recursos (por ejemplo, los efectos estacionales). La elasticidad y la escalabilidad abarcan no solo los aspectos cuantitativos del servicio, sino también la calidad y la seguridad de las medidas que deban adaptarse a los diferentes grados de sensibilidad de los datos almacenados de los clientes;

f) **combinación de recursos**: posibilidad de que el proveedor reúna recursos físicos o virtuales para atender a uno o más clientes sin que estos tengan control o conocimiento de los procesos involucrados.

Servicios de computación en la nube: servicios prestados a través de la **computación en la nube**. Varían y están en constante evolución. Pueden incluir el suministro y la utilización de la conectividad y los servicios informáticos básicos (como el servicio de almacenamiento, correos electrónicos y aplicaciones de oficina). También pueden incluir la provisión y el uso de la gama completa de la infraestructura física de tecnología de la información (como servidores y centros de datos) y los recursos virtuales necesarios para construir plataformas propias de tecnología de la información, o desplegar, gestionar y administrar las aplicaciones o los programas informáticos adquiridos o creados por los clientes. Los **IaaS, SaaS, PaaS**, etc., son tipos de servicios de computación en la nube.

Colaboradores de los servicios de computación en la nube (por ejemplo, auditores de servicios de nube, intermediarios de servicios de nube o integradores de sistemas): personas que apoyan las actividades del proveedor, del cliente o de ambos o que colaboran en esas actividades. Los auditores de nube realizan la **auditoría** de la provisión y el uso de los **servicios de computación en la nube**. Los intermediarios de servicios de nube ayudan a las partes en relación con una amplia gama de cuestiones, por ejemplo, a encontrar la solución de nube más adecuada, negociar condiciones aceptables y migrar los contenidos de los clientes a la nube.

Datos obtenidos de los servicios de nube: datos bajo control del proveedor que se obtienen como resultado del uso por el cliente de los servicios de computación en la nube de ese proveedor. Incluyen los **metadatos** y otros registros de datos generados por el proveedor que contienen información sobre quién utilizó los servicios, a qué horas y cuáles fueron las funciones y los tipos de datos utilizados. También pueden contener información sobre los usuarios autorizados, sus identificadores, y cualquier configuración, personalización y modificación que se haga.

Responsable de los datos: persona que determina los objetivos y medios que han de emplearse en el procesamiento de **datos personales**.

Requisitos de **ubicación de los datos**: requisitos relativos a la ubicación de los datos y otros contenidos, de los centros de datos, o del proveedor. Pueden prohibir que determinados datos (como los **metadatos** y las copias de seguridad) sean alojados o trasladados dentro o fuera de una zona o jurisdicción determinada, o exigir que se obtenga la autorización previa de un órgano estatal competente para ello. Suelen estar previstos en las leyes y reglamentos sobre protección de datos, los cuales pueden prohibir en particular que los **datos personales** sean alojados en jurisdicciones que no respetan determinadas normas de protección de **datos personales** o trasladados a ellas.

Procesador de los datos: persona que procesa los datos en nombre del **responsable de los datos**.

Derechos de los sujetos de los datos: derechos relacionados con los **datos personales** de los sujetos de los datos. La ley puede disponer que los sujetos de los datos tengan el derecho a ser informados de todos los hechos significativos relacionados con sus datos personales, como su ubicación, su utilización por terceros y las fugas de datos u otras infracciones relacionadas con los datos. También pueden tener el derecho a acceder en cualquier momento a sus datos personales, el derecho a que estos se eliminen (en virtud del derecho al olvido), el derecho a restringir el **procesamiento** de sus datos personales y el derecho a que esos datos sean **transferibles**.

Modelos de despliegue: diversas formas de organizar la computación en la nube sobre la base del control y el uso compartido de recursos físicos o virtuales, como las siguientes:

a) modelo de **nube pública**, en que los **servicios de computación en la nube** pueden estar a disposición de cualquier cliente interesado en ellos y los recursos son controlados por el proveedor;

b) modelo de **nube compartida**, en que los **servicios de computación en la nube** se prestan exclusivamente a un determinado grupo de clientes relacionados entre sí y con necesidades comunes, y en que los recursos son controlados por al menos uno de los miembros del grupo;

c) modelo de **nube privada**, en que los **servicios de computación en la nube** son utilizados exclusivamente por un solo cliente de esos servicios y los recursos son controlados por ese cliente;

d) modelo de **nube híbrida**, en que se utilizan por lo menos dos modelos diferentes de despliegue en la nube.

Período de interrupción o corte del servicio: tiempo durante el cual los servicios de computación en la nube no están a disposición del cliente. Ese tiempo no se tiene en cuenta en el cálculo del **período de disponibilidad**. Las tareas de mantenimiento y actualización se suelen incluir en los períodos de interrupción del servicio.

Tiempo de respuesta inicial: tiempo transcurrido entre la comunicación de un incidente por el cliente y la respuesta inicial del proveedor.

Aprovechamiento de husos horarios ("*Follow the sun*"): modelo en que el volumen de trabajo se distribuye entre diferentes lugares geográficos para equilibrar los recursos y la demanda de manera más eficiente. El propósito de este modelo puede ser prestar servicios ininterrumpidos y minimizar la distancia media entre los servidores y los usuarios finales a fin de reducir la **latencia** y aumentar al máximo la velocidad de transmisión de los datos entre dispositivos (tasa de transferencia de datos o DTR, por sus siglas en inglés, o rendimiento).

IaaS: tipos de **servicios de computación en la nube** con los que el cliente puede obtener y utilizar recursos de procesamiento, almacenamiento o de redes. El cliente no administra ni controla los recursos físicos ni virtuales, pero tiene el control de los sistemas operativos, el almacenamiento y las aplicaciones instaladas que utilicen los recursos físicos y virtuales. El cliente puede tener también una posibilidad limitada de controlar determinados componentes de red (por ejemplo, los cortafuegos locales).

Representante de la insolvencia: persona u órgano autorizado en un procedimiento de insolvencia para administrar la reorganización o la liquidación de los bienes del proveedor insolvente sometidos a dicho procedimiento.

Interoperabilidad: capacidad de dos o más sistemas o aplicaciones para intercambiar información y utilizar mutuamente la información que se intercambian.

Licencias de propiedad intelectual: acuerdos entre el titular de los derechos de propiedad intelectual (es decir, el licenciante) y la persona autorizada para utilizar esos derechos de propiedad intelectual (el licenciatario). Suelen imponer restricciones y obligaciones relativas a la medida y la forma en que el licenciatario o terceros pueden utilizar la propiedad bajo licencia. Por ejemplo, pueden concederse licencias de uso de programas informáticos y contenido visual (diseños, planos e imágenes) para un uso específico, prohibiendo la copia, la modificación o la mejora, y limitándose a un determinado soporte. Las licencias pueden limitarse a un mercado determinado (por ejemplo, nacional o (sub)regional), a un número de usuarios o pueden estar sujetas a plazos. Puede prohibirse el otorgamiento de sublicencias. El licenciante puede exigir que cada vez que se utilicen los derechos de propiedad intelectual se haga referencia al titular de dichos derechos.

Latencia: desde la perspectiva del cliente, la demora entre la solicitud del usuario y la respuesta del proveedor. Afecta a la utilidad real de los **servicios de computación en la nube**.

Servicios estratificados de computación en la nube: cuando el proveedor no es propietario de la totalidad o una parte de los recursos de computación que utiliza para la prestación de los servicios de computación en la nube a sus clientes, sino que él es, a su vez, cliente de todos o algunos de los **servicios de computación en la nube**. Por ejemplo, el proveedor de servicios **PaaS** o **SaaS** puede utilizar la infraestructura de almacenamiento y servidores (centros de datos, servidores de datos) que sean propiedad de otra entidad o sean proporcionados por esta. Como resultado de ello, podrían participar en la prestación al cliente de los servicios de computación en la nube uno o más subproveedores. El cliente quizás no sepa qué niveles participan en la prestación de los servicios en un momento dado, lo que hace difícil determinar y gestionar los riesgos. Los **servicios estratificados de computación en la nube** son comunes, especialmente en la modalidad **SaaS**.

Dependencia de la solución tecnológica ("*lock-in*"): cuando el cliente depende de un único proveedor porque el costo de cambiar a otro sería muy alto. El costo en este contexto debe entenderse en el sentido más amplio posible, de modo que abarque no solo el costo pecuniario, sino también el costo en términos de esfuerzo, tiempo y relaciones. El riesgo de dependencia de las aplicaciones y los datos puede ser elevado en los servicios **SaaS** y **PaaS**. Los datos pueden estar en formatos específicos del sistema de nube del proveedor y podrían no resultar utilizables en otros sistemas. Además, es posible que el proveedor utilice una aplicación o un sistema propio para

organizar los datos del cliente que requiera la modificación de las condiciones de la licencia para permitir el funcionamiento fuera de la red del proveedor. En el caso de los servicios **PaaS** también podría existir dependencia de las versiones de ejecución de los programas ya que estas versiones (es decir, los programas informáticos diseñados para apoyar la ejecución de programas informáticos escritos en un lenguaje de programación específico) suelen estar muy personalizadas (en lo concerniente a aspectos como la asignación o la liberación de la memoria, la depuración de errores, etc.). La dependencia de la solución tecnológica en los servicios **IaaS** varía en función de los distintos servicios de infraestructura utilizados, pero también puede dar lugar a una dependencia de aplicaciones si se depende de las características de determinadas políticas (por ejemplo, de los controles de acceso) o a una dependencia de datos si se traslada a la nube un mayor número de datos para su almacenamiento.

Metadatos: información básica sobre los datos (como su autor, su fecha de creación, de modificación y el tamaño del archivo). Hacen que resulte más sencillo encontrar y utilizar los datos y pueden ser necesarios para garantizar la autenticidad de los registros a lo largo del tiempo. Pueden ser generados por el cliente o el proveedor.

PaaS: tipos de **servicios de computación en la nube** con los que el cliente puede desplegar, gestionar y administrar en la nube aplicaciones o programas informáticos creados o adquiridos por él utilizando alguno o algunos de los lenguajes de programación y entornos de ejecución soportados por el proveedor.

Parámetros de desempeño: parámetros cuantitativos (con objetivos, indicadores o rangos de valores de desempeño numéricos) y cualitativos (con garantías de calidad de los servicios). Pueden medir la conformidad con las normas aplicables, incluida la fecha de vencimiento de los certificados de conformidad. Para que tengan sentido, deberían tener por objeto evaluar los aspectos del desempeño que sean importantes para el cliente y deberían hacerlo de una manera sencilla y verificable. Pueden ser diferentes en función de los riesgos y de las necesidades del negocio (por ejemplo, la importancia crítica de determinados datos, servicios o aplicaciones y las correspondientes prioridades de recuperación). Por ejemplo, un sistema no esencial diseñado para utilizar la nube con fines de archivo no necesitaría el mismo **período de disponibilidad** u otras condiciones del **SLA** que las operaciones esenciales o las operaciones en tiempo real.

Permanencia del almacenamiento de los datos: probabilidad de que los datos almacenados en la nube no se pierdan durante la vigencia del contrato. Puede reflejarse en el contrato como un objetivo mensurable que el cliente utilizará para evaluar las medidas puestas en marcha por el proveedor para garantizar que los datos permanezcan almacenados.

Datos personales: datos que pueden utilizarse para identificar a la persona física a la que se refieren esos datos. La definición de los datos personales en algunas jurisdicciones puede abarcar cualquier dato o información directa o indirectamente vinculada o relacionada con una persona identificada o identificable (el **sujeto de los datos**).

Procesamiento [de datos personales]: la recopilación, el registro, la organización, el almacenamiento, la adaptación o la alteración, la recuperación, la consulta, la utilización, la revelación por transmisión, la difusión o cualquier otra forma de puesta a disposición, alineación o combinación, bloqueo, eliminación o destrucción de los datos.

Portabilidad: capacidad para transferir datos, aplicaciones y otros contenidos de un sistema a otro fácilmente (es decir, a bajo precio, con el menor trastorno posible y sin necesidad de volver a introducir los datos, reorganizar los procesos o reprogramar las aplicaciones). Esto podría lograrse si fuera posible recuperar los datos en un formato que es aceptado por otro sistema o con una transformación simple y directa utilizando instrumentos normalmente disponibles.

Medidas posteriores al incidente: medidas que deben adoptar el proveedor, el cliente o ambos, después de un incidente de seguridad, incluso haciendo intervenir a un tercero. Pueden incluir el aislamiento o la puesta en cuarentena de las zonas afectadas, la realización de análisis de las causas profundas del incidente y la elaboración por el afectado, juntamente con la otra parte, o por un tercero independiente, de un informe de análisis del incidente.

Objetivos de punto de recuperación (RPO, por sus siglas en inglés): período máximo anterior a una interrupción imprevista de los servicios durante el cual pueden perderse los cambios realizados en los datos como consecuencia de la recuperación. Si se especifica en el contrato un RPO de las dos horas anteriores a la interrupción de los servicios, ello significa que tras la recuperación se podrá acceder a todos los datos en la forma que tenían dos horas antes de producirse la interrupción.

Objetivos de tiempo de recuperación (RTO, por sus siglas en inglés): período de tiempo máximo que tardarán en recuperarse todos los servicios de computación en la nube y todos los datos tras producirse una interrupción imprevista.

Reversibilidad: proceso que debe seguirse para que el cliente recupere de la nube sus datos, aplicaciones y otros contenidos relacionados y para que el proveedor elimine los datos y otros contenidos conexos del cliente después del plazo acordado.

SaaS: aquellos tipos de **servicios de computación en la nube** con los que el cliente puede utilizar las aplicaciones en la nube del proveedor.

Regulación por sectores: regulación de los sectores financiero, sanitario o público o de otros sectores o profesiones (por ejemplo, el secreto profesional que deben guardar los abogados y los médicos) y las normas para el manejo de la información clasificada (entendida en sentido amplio como información de acceso restringido por ley o reglamento a determinadas categorías de personas).

Notificación de incidentes de seguridad: notificación hecha a las partes afectadas, a las autoridades del Estado o al público en general acerca de un incidente de seguridad. Puede comprender las circunstancias y la causa del incidente, el tipo de datos afectados, las medidas que deben adoptarse para resolver el incidente, el plazo en que se espera resolverlo y los planes de contingencia que se han de emplear mientras se lo resuelve. Puede incluir también información sobre quebrantamientos de la seguridad que no han tenido éxito, los ataques contra objetivos concretos (por usuario del cliente, por aplicación específica, por cada máquina física concreta), tendencias y estadísticas.

Acuerdo sobre las características de los servicios (SLA, por sus siglas en inglés): aquella parte del contrato de computación en la nube firmado por el proveedor y el cliente en que se describen los servicios de computación en la nube previstos en el contrato y la forma en que deben prestarse (**parámetros de desempeño**) [*cross-link*].

Soluciones de nube genéricas y estandarizadas para múltiples suscriptores: servicios de computación en la nube prestados a un número ilimitado de clientes como producto masivo o básico en condiciones uniformes y no negociables determinadas por el proveedor. En este tipo de soluciones es habitual encontrar amplios descargos y eximentes de responsabilidad del proveedor. El cliente quizás pueda comparar diferentes proveedores y sus contratos y seleccionar entre los disponibles en el mercado aquel que más se adecue a sus necesidades, pero no puede negociar el contrato.

Período de disponibilidad del servicio: tiempo durante el cual es posible acceder a los servicios de computación en la nube y utilizarlos.

Información **escrita o por escrito**: información que debe estar accesible para que resulte utilizable en una referencia posterior. Abarca tanto la información en papel como las comunicaciones electrónicas. “Accesible” significa que la información en formato electrónico debe poder leerse e interpretarse, y que los programas que pudieran ser necesarios para que esa información pueda leerse deben conservarse. “Utilizable” se refiere tanto a la utilización de la información por el ser humano como a su procesamiento informático.