CNUDMI
COMISIÓN DE LAS NACIONES UNIDAS
PARA EL DERECHO MERCANTIL INTERNACIONAL

Notas sobre las principales cuestiones relacionadas con los contratos de computación en la nube

(preparadas por la secretaría de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, 2019)

NACIONES UNIDAS

Puede obtenerse más informción de

la secretaría de la CNUDMI, Centro Internacional de Viena,
apartado postal 500, 1400 Viena (Austria)

Teléfono: (+43-1) 26060-4060
Telefax: (+43-1) 26060-5813
Internet: uncitral.un.org
Correo electrónico: uncitral@un.org

COMISIÓN DE LAS NACIONES UNIDAS
PARA EL DERECHO MERCANTIL INTERNACIONAL

Notas sobre las principales cuestiones relacionadas con los contratos de computación en la nube

(preparadas por la secretaría de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, 2019)

NACIONES UNIDAS
Nueva York, 2019

Prefacio

En sus períodos de sesiones 47º a 50º, celebrados entre 2014 y 2017, la CNUDMI examinó el tema de los aspectos contractuales de la computación en la nube sobre la base de las propuestas presentadas por el Canadá (A/CN.9/823 y A/CN.9/856), los informes sobre la marcha de la labor del Grupo de Trabajo IV (Comercio Electrónico) y los informes orales de la Secretaría[1], y pidió a la Secretaría y al Grupo de Trabajo que realizaran una labor preparatoria sobre ese tema[2].

El Grupo de Trabajo examinó el tema en detalle en su 55º período de sesiones (Nueva York, 24 a 28 de abril de 2017) sobre la base de una nota de la Secretaría (A/CN.9/WG.IV/WP.142) y, en su 56º período de sesiones (Nueva York, 16 a 20 de abril de 2018), a partir de un proyecto de lista de verificación sobre los aspectos contractuales de la computación en la nube preparado con la colaboración de expertos, en particular durante una reunión de un grupo de expertos convocada por la Secretaría y celebrada en Viena los días 20 y 21 de noviembre de 2017 (A/CN.9/WG.IV/WP.148). En su 52º período de sesiones, celebrado en 2019, la CNUDMI, conforme a la decisión que había adoptado en su 51er período de sesiones de examinar el proyecto de notas preparado por la Secretaría sobre las principales cuestiones relacionadas con los contratos de computación en la nube antes de su publicación[3], aprobó la publicación de las notas, con las modificaciones introducidas durante el período de sesiones, en forma de notas de la Secretaría y en los seis idiomas oficiales de las Naciones Unidas, como instrumento de consulta en línea y como folleto impreso y electrónico[4].

En la presente publicación se reproducen las *Notas sobre las principales cuestiones relacionadas con los contratos de computación en la nube* en la forma en que las aprobó la CNUDMI para su publicación en 2019.

---

[1] *Documentos Oficiales de la Asamblea General, sexagésimo noveno período de sesiones, Suplemento núm. 17* (A/69/17), párr. 150; *ibid., septuagésimo período de sesiones, Suplemento núm. 17* (A/70/17), párr. 358; e *ibid., septuagésimo primer período de sesiones, Suplemento núm. 17* (A/71/17), párr. 229.

[2] *Ibid., septuagésimo primer período de sesiones, Suplemento núm. 17* (A/71/17), párrs. 235 y 353; e *ibid., septuagésimo segundo período de sesiones, Suplemento núm. 17* (A/72/17), párr. 127.

[3] *Ibid., septuagésimo tercer período de sesiones, Suplemento núm. 17* (A/73/17), párr. 150.

[4] *Ibid., septuagésimo cuarto período de sesiones, Suplemento núm. 17* (A/74/17), párr. 151.

Índice

Introducción

1. En estas *Notas* se abordan las principales cuestiones relacionadas con los contratos de computación en la nube celebrados entre entidades mercantiles en los que una de las partes (el proveedor) presta a la otra (el cliente) uno o más **servicios de computación en la nube** para su uso final. Los contratos de reventa u otras formas de distribución ulterior de los **servicios de computación en la nube** están excluidos del ámbito de aplicación de las *Notas*. También quedan excluidos de su ámbito de aplicación los contratos celebrados con **colaboradores de los servicios de computación en la nube** y otros terceros que pudieran participar en la prestación de esos servicios al cliente (por ejemplo, los contratos celebrados con subcontratistas o proveedores de servicios de Internet).

2. En función de lo que disponga la legislación aplicable, los contratos de computación en la nube pueden considerarse contratos de servicios, de arrendamiento, de externalización, de licencia, mixtos o de otro tipo, y los requisitos legales en cuanto a su forma y contenido pueden variar según la naturaleza que se les asigne. En algunas jurisdicciones, las propias partes pueden atribuir a su contrato una determinada naturaleza cuando la legislación guarde silencio o sea ambigua respecto de la cuestión, en cuyo caso los órganos jurisdiccionales tendrán en cuenta la naturaleza asignada al contrato al interpretar sus cláusulas, a menos que ello sea contrario a la ley, la práctica judicial, la verdadera intención de las partes, las circunstancias de hecho o las costumbres o prácticas comerciales.

3. En estas *Notas* se abordan cuestiones que pueden plantearse con respecto a los contratos de computación en la nube con independencia del tipo de **servicios de computación en la nube** de que se trate (por ejemplo, de **infraestructura como servicio** (**IaaS**), **plataforma como servicio** (**PaaS**) o **programas informáticos como servicio** (**SaaS**)), de su **modelo de despliegue** (por ejemplo, **público, compartido, privado** o **híbrido**) y de las condiciones de pago (con o sin remuneración) que se apliquen. Las *Notas* se centran principalmente en los contratos de servicios de computación en la nube de tipo **SaaS** que utilizan el modelo de nube pública y se prestan a cambio de una remuneración.

4. La posibilidad de negociar las cláusulas de un contrato de computación en la nube dependerá de muchos factores, en particular de si el contrato versa sobre **soluciones de nube genéricas y estandarizadas para múltiples**

suscriptores o sobre una solución individual hecha a medida, de si existen o no ofertas de competidores, y de las posiciones de negociación de los posibles contratantes futuros. La posibilidad de negociar las condiciones de un contrato, especialmente las cláusulas relativas a su suspensión, resolución o modificación unilaterales por el proveedor y las cláusulas de responsabilidad, puede ser un factor importante a la hora de elegir un proveedor en caso de que existan varias alternativas. Aunque las *Notas* se hayan elaborado principalmente para las partes que negocian un contrato de computación en la nube, también pueden resultar útiles para los clientes que deseen revisar las condiciones estándar ofrecidas por los proveedores a fin de determinar si esas condiciones se ajustan a sus necesidades.

5. Las *Notas* no deben considerarse una fuente de información exhaustiva sobre la redacción de contratos de computación en la nube ni un sustituto del asesoramiento jurídico y técnico o de los servicios de asesores profesionales. En estas *Notas* se señalan algunas cuestiones que deberían tener en cuenta quienes consideren la posibilidad de celebrar un contrato, tanto antes de su redacción como durante esta, entre ellas la responsabilidad compartida de las partes con respecto a las medidas de seguridad, sin que se pretenda transmitir la idea de que todas esas cuestiones deben analizarse siempre. Las diversas soluciones que se examinan en las *Notas* no se aplicarán a las relaciones entre las partes a menos que estas las acepten expresamente o que las soluciones resulten de lo dispuesto en la ley aplicable. Ni los títulos ni los subtítulos utilizados en estas *Notas* ni el orden en que aparecen deben considerarse obligatorios ni debe entenderse que indican una preferencia por una estructura o un estilo determinados 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 y requisitos legales, así como en función de las necesidades y preferencias de las partes.

6. Por último, estas *Notas* no deben entenderse como una expresión de la opinión de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) ni de su secretaría sobre la conveniencia de celebrar contratos de computación en la nube.

7. Las *Notas* constan de dos partes y un glosario: en la primera parte se examinan los principales aspectos precontractuales que las futuras partes quizás deseen tener en cuenta antes de celebrar un contrato de computación en la nube; en la segunda se abordan las principales cuestiones contractuales que las partes en la negociación pueden tener que 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 de verificación a fin de facilitar su comprensión.

Primera parte. Principales aspectos precontractuales

A. VERIFICACIÓN DE LA EXISTENCIA DE NORMAS LEGALES IMPERATIVAS Y OTROS REQUISITOS

8. El régimen legal aplicable al cliente, al proveedor o a ambos puede imponer ciertas condiciones para la celebración de un contrato de computación en la nube. Esas condiciones también pueden tener su origen en obligaciones contractuales, como las que surgen de las **licencias de propiedad intelectual (PI).** Las partes deberían prestar especial atención a las leyes y reglamentos en materia de **datos personales**, protección del consumidor, ciberseguridad, control de las exportaciones, aduanas, impuestos y secretos comerciales, a la reglamentación específica en materia de PI y a la **normativa propia de cada sector** que pudieran serles aplicables a ellas mismas y a su futuro contrato. El incumplimiento de los requisitos obligatorios puede acarrear importantes consecuencias negativas, entre ellas la nulidad o la inexigibilidad de la totalidad o una parte del contrato, la imposición de multas administrativas y la responsabilidad penal.

9. Las condiciones exigidas para celebrar un contrato de computación en la nube pueden variar según el sector y la jurisdicción de que se trate. Por ejemplo, puede requerirse la adopción de medidas especiales para proteger los **derechos de los sujetos de los datos**, el despliegue de un determinado modelo (por ejemplo, **nube privada** en lugar de **pública**), el cifrado de los datos alojados en la nube y el registro ante organismos públicos de una operación o un programa informático utilizado en el procesamiento de los **datos personales**. También pueden exigirse **requisitos de ubicación de los datos**, así como otras condiciones relacionadas con el proveedor.

Ubicación de los datos

10. Los **requisitos de ubicación de los datos** pueden derivarse en particular de la legislación aplicable a los **datos personales**, los datos contables y los datos del sector público, así como de las leyes y reglamentos de fiscalización de las exportaciones que pueden limitar la transmisión de determinados programas informáticos o información hacia o desde determinados países o

regiones. Será de suma importancia para las partes cumplir los **requisitos de ubicación de los datos** establecidos en la ley aplicable, los que no podrán dejarse sin efecto por la vía del contrato.

11. Los **requisitos de ubicación de los datos** también pueden emanar de obligaciones contractuales (por ejemplo, **licencias de PI** en las que se exija que el contenido bajo licencia se almacene en los servidores seguros del propio usuario). También es posible que se prefiera establecer **requisitos de ubicación de los datos** por razones puramente prácticas, por ejemplo, para reducir la **latencia**, lo que puede ser especialmente importante en las operaciones en tiempo real, como las de tipo bursátil. (En cuanto a las medidas de salvaguardia que pueden incluirse en el contrato respecto de la ubicación de los datos, véase la segunda parte, párrs. 74, 75 y 78).

Elección de la parte contratante

12. La elección de una parte contratante puede estar limitada no solo por las condiciones del mercado sino también por disposición de la ley. Es posible que exista una prohibición legal de celebrar contratos de computación en la nube con personas o entidades extranjeras, de determinadas jurisdicciones o que no hayan sido acreditadas ante los organismos públicos competentes o no hayan recibido certificación de estos. También puede supeditarse la prestación de **servicios de computación en la nube** por parte de una persona o entidad extranjera en una jurisdicción determinada a que esa persona o entidad constituya una empresa mixta con una entidad nacional u obtenga determinadas licencias y permisos locales, entre ellos permisos de exportación. En la elección de la parte contratante también pueden influir los **requisitos de ubicación de los datos** (véanse los párrs. 10 y 11 *supra*), así como las disposiciones legales por las que se obligue a alguna de las partes a comunicar datos y otros contenidos a organismos públicos extranjeros o a facilitar el acceso de esos organismos a dichos datos o contenidos.

B. EVALUACIÓN PRECONTRACTUAL DE LOS RIESGOS

13. Las normas imperativas de la ley aplicable pueden exigir que se realice una evaluación de los riesgos como condición para celebrar un contrato de computación en la nube. Aun cuando la ley no imponga ese requisito, las partes pueden decidir llevar a cabo una evaluación de los riesgos que quizás les permita encontrar estrategias para mitigarlos, entre ellas la negociación de determinadas cláusulas contractuales.

14. No todos los riesgos derivados de los contratos de computación en la nube están relacionados específicamente con la nube. Respecto de algunos de ellos (por ejemplo, los riesgos derivados de las interrupciones de la conexión a Internet) habrá que tomar medidas fuera del marco de un contrato de computación en la nube, y no todos los riesgos podrán mitigarse a un costo aceptable (por ejemplo, el riesgo de deterioro de la reputación). Además, la evaluación de los riesgos no es por lo general una medida que se adopte una sola vez antes de celebrar un contrato. Es posible que los riesgos se evalúen continuamente durante el período de vigencia del contrato y que, a raíz de esas evaluaciones, sea necesario modificar el contrato o ponerle fin.

Verificación de la información sobre determinados servicios de computación en la nube y una determinada parte contratante

15. La siguiente información puede resultar de interés para las partes cuando consideren la posibilidad de utilizar un determinado **servicio de computación en la nube** en particular y elegir a una parte contratante:

a) las **licencias de PI** necesarias para utilizar un determinado servicio de computación en la nube;

b) las políticas de privacidad, confidencialidad y seguridad existentes, en especial en lo que respecta a la prevención del acceso, la utilización, la alteración o la destrucción no autorizados de los datos durante su procesamiento, tránsito o transmisión mediante el uso de infraestructura de computación en la nube;

c) las medidas destinadas a garantizar el acceso continuado a los **metadatos**, registros de auditoría y otros registros que muestren las medidas de seguridad adoptadas;

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

e) las políticas aplicables a la prestación de asistencia en los procesos de migración a la nube y finalización del servicio, así como en materia de **interoperabilidad** y **portabilidad**;

f) los métodos actuales de investigación de antecedentes y capacitación de los empleados, subcontratistas y otros terceros que participen en la prestación de los servicios de computación en la nube;

g) las estadísticas relativas a los **incidentes de seguridad** y la información cuantitativa y cualitativa sobre los servicios prestados en anteriores procedimientos de recuperación en casos de desastre;

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

i) la información sobre la periodicidad y el alcance de la auditoría realizada por un órgano independiente;

j) la viabilidad financiera;

k) las pólizas de seguro;

l) los posibles conflictos de intereses;

m) el alcance de la subcontratación y de los **servicios estratificados de computación en la nube**;

n) el grado de aislamiento de los datos y otros contenidos en la infraestructura de computación en la nube; y

o) las funciones que cada parte espera que asuma la otra y la responsabilidad compartida por las partes con respecto a las medidas de seguridad.

Riesgo de que se vulneren derechos de PI

16. Puede existir el riesgo de que se vulneren derechos de PI en los casos en que, por ejemplo, el proveedor no sea el propietario de los recursos que suministra a sus clientes ni quien los ha desarrollado, sino que los utilice en virtud de un acuerdo de **licencia de PI** celebrado con un tercero. También puede surgir dicho riesgo cuando, para llevar a efecto lo estipulado en el contrato, se exige al cliente que otorgue al proveedor una licencia de uso del contenido que el cliente desea almacenar en la nube. En algunas jurisdicciones, el almacenamiento de contenido en la nube, incluso con el fin de hacer copias de seguridad, puede considerarse una reproducción y requerir la autorización previa del titular de los derechos de PI.

17. Convendrá a los intereses de ambas partes asegurarse, antes de firmar el contrato, de que el uso de los servicios de computación en la nube no constituirá una violación de derechos de PI ni una causal de revocación de las licencias concedidas a cualquiera de las partes. El costo de incurrir en una violación de derechos de PI puede ser muy elevado. Es posible que sea necesario pactar el derecho a conceder sublicencias, o celebrar directamente con el correspondiente tercero licenciante un contrato de licencia por el que se otorgue el derecho a gestionar las licencias. Para utilizar programas informáticos de código abierto u otros contenidos tal vez haya que obtener previamente el consentimiento de terceros y revelar el código fuente con las modificaciones introducidas en esos programas y otros contenidos.

Riesgos para la seguridad, la integridad, la confidencialidad y la privacidad de los datos

18. Cuando se realiza la migración total o parcial de los datos a la nube, el cliente pierde tanto el control exclusivo de los datos como la capacidad de aplicar las medidas necesarias para garantizar la integridad y la confidencialidad de los datos o verificar si estos se están procesando y conservando correctamente. El grado de pérdida de control dependerá del tipo de **servicios de computación en la nube.**

19. Debido a las características inherentes a los **servicios de computación en la nube**, como el **acceso amplio a la red**, el **arrendamiento múltiple** y la **combinación de recursos**, es posible que las partes tengan que adoptar más precauciones para evitar la interceptación de las comunicaciones y otras formas de ciberataque que puedan dar lugar a la pérdida o alteración de las credenciales de acceso a los servicios de computación en la nube, la pérdida de datos y otras violaciones de la seguridad. El aislamiento adecuado de los recursos, la segregación de los datos y la adopción de procedimientos de seguridad rigurosos son especialmente importantes en entornos compartidos como el de la computación en la nube.

20. La adopción de medidas de seguridad será una responsabilidad compartida por las partes en el entorno de la computación en la nube, independientemente del tipo de servicios de computación en la nube que se utilicen. La evaluación de los riesgos en la etapa precontractual ofrece una buena oportunidad para que las partes eliminen cualquier ambigüedad que pueda existir en la definición de sus funciones y responsabilidades en lo que respecta a la seguridad, la integridad, la confidencialidad y la privacidad de los datos. Las cláusulas del contrato serán importantes para reflejar lo acordado por las partes en cuanto a la distribución de los riesgos y las responsabilidades entre ellas en relación con esos y otros aspectos de la prestación de servicios de computación en la nube (véase la segunda parte, párrs. 125 a 137). Sin embargo, dichas cláusulas no podrán dejar sin efecto las disposiciones imperativas de la ley.

Pruebas de penetración, auditorías e inspecciones in situ

21. En la etapa precontractual pueden adoptarse medidas para verificar que el aislamiento de los recursos, la segregación de los datos, los procedimientos de identificación y otras medidas de seguridad sean adecuados. Tales medidas deberían estar dirigidas a determinar las posibles precauciones adicionales que las partes quizás deban adoptar para prevenir violaciones de la seguridad de los datos y otros problemas de funcionamiento en la prestación de los servicios de computación en la nube al cliente.

22. Los centros de datos que se utilizan para prestar **servicios de computación en la nube** pueden tener que someterse, por disposición legal o reglamentaria, a **auditorías**, pruebas de penetración e inspecciones físicas, especialmente para verificar que el lugar en que se encuentran se ajusta a los **requisitos de ubicación de los datos** previstos en la ley (véanse los párrs. 10 y 11 *supra*). Las partes tendrán que ponerse de acuerdo sobre las condiciones en que se llevarán a cabo esas actividades, en particular el momento en que se realizarán, la forma en que se distribuirán los gastos y la indemnización que deberá pagarse en caso de que se produzcan daños como resultado de esas actividades.

Riesgos de dependencia

23. Una de las cuestiones más importantes que las partes deberían tener en cuenta es la de evitar o reducir los riesgos de **dependencia** que suelen derivarse de la falta de **interoperabilidad** y **portabilidad**. En los contratos a largo plazo, así como en los contratos a corto y mediano plazo que se renuevan automáticamente, el riesgo de dependencia puede ser mayor.

24. Los riesgos de dependencia de las aplicaciones y los datos son especialmente elevados en los servicios de tipo **Saas** y **PaaS**. Los datos pueden estar en formatos específicos de un sistema de nube que no sean utilizables en otros sistemas. Además, es posible que la aplicación o el sistema utilizados para organizar los datos estén patentados y que, por lo tanto, sea necesario modificar las condiciones de la licencia para permitir el funcionamiento en una red diferente. En los casos en que se hayan elaborado programas a fin de interactuar con las interfaces de programación de aplicaciones (API), puede ser necesario volver a escribir el programa para tener en cuenta la API del nuevo sistema. Esos cambios también pueden entrañar gastos elevados como consecuencia de la necesidad de volver a capacitar a los usuarios finales.

25. En el caso de los servicios **PaaS,** también podría existir dependencia de las versiones de ejecución de los programas, ya que esas 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 (por ejemplo, en lo concerniente a aspectos como la asignación o la liberación de memoria, la depuración de errores, etc.). En lo que respecta a los servicios **IaaS**, la dependencia varía en función de los servicios de infraestructura específicos que se utilicen, aunque, al igual que los servicios PaaS, algunos servicios de infraestructura también pueden dar lugar a una dependencia de las aplicaciones si el servicio depende de determinados aspectos de política (por ejemplo, de los controles de acceso). Algunos servicios de infraestructura también pueden dar lugar a una depen-

dencia de los datos si se traslada a la nube un mayor volumen de datos para su almacenamiento.

26. En la etapa precontractual podrían realizarse pruebas para verificar si los datos y otros contenidos pueden exportarse a otro sistema y ser utilizables en él. Es posible que sea necesario sincronizar las plataformas internas del cliente con las que están en la nube y reproducir los datos en otro lugar. Una estrategia importante para mitigar los riesgos de **dependencia** puede ser la de contratar con más de una parte y optar por una combinación de diversos tipos de **servicios de computación en la nube** y sus **modelos de despliegue** (por ejemplo, emplear múltiples proveedores), aunque ello podría repercutir en los costos y acarrear otras consecuencias. Algunas cláusulas contractuales también pueden ayudar a mitigar los riesgos de dependencia (véase la segunda parte, en particular los párrs. 84 a 86 y 144).

Riesgos para la continuidad de las operaciones

27. Los riesgos relacionados con la continuidad de las operaciones pueden preocupar a las partes no solo cuando se acerca la fecha prevista de vencimiento del contrato, sino también cuando existe la posibilidad de que se produzca una suspensión unilateral o una resolución anticipada del contrato, en particular en el caso de que alguna de las partes cese en sus actividades comerciales. Es posible que la ley exija que se adopte de antemano una estrategia adecuada que garantice la continuidad de las operaciones, especialmente para evitar las consecuencias negativas de la cancelación o la suspensión de los servicios de computación en la nube para los usuarios finales. La inclusión de determinadas cláusulas en el contrato también puede ayudar a mitigar los riesgos para la continuidad de las operaciones (véase la segunda parte, párrs. 109 a 111, 114, 115, 153, 173 y 182).

Estrategias de salida

28. Para que las estrategias de salida sean eficaces, las partes quizás tengan que aclarar desde el principio: *a)* el contenido al que podrá darse salida (por ejemplo, únicamente los datos que el cliente haya subido a la nube o también los **datos obtenidos de los servicios de nube**); *b)* las modificaciones que será necesario realizar en las **licencias de PI** para permitir el uso de ese contenido en otro sistema; *c)* el control de las claves de descifrado y el acceso a ellas; y *d)* el tiempo necesario para completar la salida. Las cláusulas contractuales relativas a la finalización del servicio suelen reflejar el acuerdo alcanzado por las partes respecto de esas cuestiones (véase la segunda parte, párrs. 157 a 167).

C. OTRAS CUESTIONES PRECONTRACTUALES

Revelación de información

29. Es posible que la legislación aplicable exija que las futuras partes contratantes se suministren recíprocamente información que les permita tomar una decisión fundamentada sobre la celebración del contrato. La falta de comunicación clara a la otra parte de la información necesaria para que el objeto de las obligaciones quede determinado o sea susceptible de determinarse antes de que se celebre el contrato puede acarrear la nulidad de la totalidad o una parte de este, o dar derecho a la parte perjudicada a reclamar una indemnización por daños y perjuicios.

30. En algunas jurisdicciones, la información precontractual puede considerarse parte integrante del contrato. En tales casos, las partes deberían asegurarse de que esa información quede debidamente registrada y evitar cualquier discrepancia entre ella y el contenido del propio contrato. Las partes tendrían que ocuparse también de las cuestiones relacionadas con los efectos que la información revelada en la etapa precontractual puede tener sobre la flexibilidad y la innovación en la fase de ejecución del contrato.

Confidencialidad

31. Es posible que parte de la información revelada en la etapa precontractual se considere confidencial, especialmente la relativa a las medidas de seguridad, identificación y autenticación, los subcontratistas, la clase de centros de datos de que se trata y el lugar en que se encuentran (lo que a su vez puede permitir identificar el tipo de datos almacenados en esos centros y los organismos públicos locales o extranjeros que tienen acceso a dichos datos). Las partes pueden convenir en que determinada información revelada en la etapa precontractual se trate de manera confidencial. Tal vez también se exija que los terceros que participan en el proceso de diligencia debida anterior a la celebración del contrato (por ejemplo, los auditores) se comprometan por escrito a mantener la confidencialidad o firmen acuerdos de no divulgación.

Migración a la nube

32. Antes de migrar datos a la nube se suele pedir al cliente que clasifique los datos que va a migrar, los asegure en función de su grado de confidencialidad e importancia e informe al proveedor sobre el nivel de protección necesario para cada tipo de datos. Es posible que el cliente también deba proporcionar al proveedor otro tipo de información necesaria para la prestación de los ser-

vicios (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).

33. Además de la transmisión de datos y otros contenidos a la nube del proveedor, la migración a la nube puede entrañar la adopción de procedimientos de instalación, configuración, cifrado y prueba, así como la capacitación del personal del cliente y otros usuarios finales. Esos aspectos pueden preverse en el contrato celebrado entre el cliente y el proveedor o en otro contrato independiente que el cliente suscriba con el proveedor o terceros, como **colaboradores de los servicios de computación en la nube**. Pueden surgir gastos adicionales. Las partes que participan en la migración suelen ponerse de acuerdo sobre las funciones y responsabilidades que les incumbirán durante ese proceso, las condiciones de su participación, el formato en que se migrarán los datos u otros contenidos a la nube, el calendario de la migración, el procedimiento de aceptación que se utilizará para confirmar 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 contractual

34. El principio ampliamente reconocido de la libertad contractual en las operaciones comerciales permite a las partes celebrar contratos y determinar su contenido. Las disposiciones legales sobre condiciones no negociables que se aplican a determinados tipos de contratos o las normas que penalizan la vulneración de derechos y las conductas contrarias al orden público, a la moral, etc., pueden imponer restricciones a la libertad contractual. Las consecuencias del incumplimiento de esas restricciones pueden ir desde la imposibilidad de exigir el cumplimiento de la totalidad o una parte del contrato hasta la posibilidad de incurrir en responsabilidad civil, administrativa o penal.

La formación del contrato

35. 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 legales que las vincularán durante el período de vigencia del contrato y, si así fuera, determinar el momento en que alcanzaron dicho acuerdo. La ley aplicable puede exigir que se cumplan determinadas condiciones para que la propuesta de celebrar un contrato se considere una oferta definitiva y vinculante (por ejemplo, que la propuesta sea suficientemente precisa en lo que respecta a los servicios de computación en la nube comprendidos en el contrato y a las condiciones de pago).

36. El contrato se considera celebrado cuando se acepta la oferta. Los mecanismos de aceptación pueden ser diversos (por ejemplo, la aceptación puede consistir, en el caso del cliente, en marcar una casilla de una página web, registrarse en línea para acceder a un servicio de computación en la nube, comenzar a utilizar servicios de este tipo o pagar un precio por ellos; en el caso del proveedor, en empezar a prestar los servicios o continuar haciéndolo; y, para ambas partes, en la firma de un contrato en línea[1] o en papel). Los cambios sus-

[1] Véanse los textos de la CNUDMI que regulan las firmas electrónicas, a saber, la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales

tanciales en la oferta (por ejemplo, los relativos a la responsabilidad, la calidad y la cantidad de los servicios de computación en la nube que han de prestarse o las condiciones de pago) pueden constituir una contraoferta que deberá recibir la aceptación de la otra parte para que el contrato se considere celebrado.

37. 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 que se exige la aceptación expresa previa). En esos casos, puede haber poco o ningún margen para negociar y modificar la oferta estándar, ya que el único paso necesario para celebrar el contrato consiste en hacer clic en "Acepto", "OK" o "De acuerdo". Cuando se negocia un contrato, su formación puede abarcar una serie de etapas, entre ellas el intercambio de información preliminar, las negociaciones, la formulación y aceptación de una oferta y la preparación del contrato.

La forma del contrato

38. Los contratos de computación en la nube suelen celebrarse en línea. Pueden recibir diferentes denominaciones (contrato de servicios de computación en la nube, contrato marco de servicios o condiciones de servicio) y pueden abarcar uno o varios documentos, como una **política de uso aceptable** (**PUA**), un **acuerdo de prestación de servicios** (**SLA**), un acuerdo de procesamiento de datos o una política de protección de datos, una política de seguridad y un contrato de licencia.

39. Las normas jurídicas aplicables a los contratos de computación en la nube pueden exigir que estos consten por **escrito** (especialmente cuando en ellos se prevea el **procesamiento de datos personales**) y que se adjunten al contrato principal todos los documentos incorporados a él por remisión. Incluso en los casos en que no se exige la forma **escrita**, las partes pueden decidir celebrar el contrato por **escrito** incorporando, asimismo, todos los acuerdos complementarios, para facilitar su consulta y en aras de la claridad, integridad, exigibilidad y eficacia del contrato.

40. La ley aplicable puede exigir que se firme un contrato en papel a determinados efectos, por ejemplo, de índole fiscal, aunque este requisito es cada vez menos frecuente debido a la disminución del uso del papel.

(Nueva York, 2005), la Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996) y la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (2001). Véase también un texto explicativo preparado por la secretaría de la CNUDMI titulado "Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas (2007)", publicado en https://uncitral.un.org/es/texts/ecommerce.

Definiciones y terminología

41. Los contratos de computación en la nube, por la naturaleza de los **servicios de computación en la nube** a que se refieren, contienen necesariamente numerosos términos técnicos. Se puede incluir en el contrato un glosario de términos, así como las definiciones de los principales términos empleados en él, a fin de evitar ambigüedades en su interpretación. Las partes tal vez deseen considerar la posibilidad de utilizar la terminología establecida a nivel internacional a fin de garantizar la coherencia y la claridad jurídica.

Contenido habitual del contrato

42. En todo contrato se suele establecer lo siguiente: *a)* la identificación de las partes contratantes; *b)* la definición del objeto y el ámbito de aplicación del contrato; *c)* la descripción de los derechos y obligaciones de las partes, en particular las condiciones de pago; *d)* el período de vigencia del contrato y las condiciones de su extinción o renovación; *e)* los recursos de que se dispondrá en caso de incumplimiento y las exenciones de responsabilidad; y *f)* los efectos de la resolución del contrato. También es habitual incluir en el contrato cláusulas relativas a la solución de controversias y a la elección del foro y la ley aplicable. El contenido, el estilo y la estructura de los contratos pueden variar considerablemente según las diversas tradiciones jurídicas, estilos de redacción y requisitos legales, así como en función de las necesidades y preferencias de las partes.

B. IDENTIFICACIÓN DE LAS PARTES CONTRATANTES

43. La correcta identificación de las partes contratantes puede incidir directamente en la formación y la exigibilidad del contrato. La ley aplicable suele especificar la información necesaria para determinar si una entidad mercantil tiene personalidad jurídica y capacidad para contratar. También puede exigir que se incluya información adicional para determinados fines, por ejemplo, un número de identificación fiscal o un poder de representación que permita determinar si una persona física tiene facultades para firmar y contraer obligaciones en nombre de una persona jurídica.

C. DEFINICIÓN DEL OBJETO Y ÁMBITO DE APLICACIÓN DEL CONTRATO

44. Habida cuenta de la diversidad de **servicios de computación en la nube** que existe, el objeto de los contratos de computación en la nube varía sustan-

cialmente en lo que se refiere a su tipología y complejidad. El objeto de un contrato puede variar a lo largo de su período de vigencia, ya que es posible que se cancelen algunos **servicios de computación en la nube** y que se añadan otros. Asimismo, el objeto de estos contratos puede abarcar la prestación de servicios esenciales, auxiliares y opcionales.

45. En la descripción del objeto del contrato se suele describir el tipo de servicios de computación en la nube que se prestarán (**SaaS, PaaS, IaaS** o una combinación de ellos), su **modelo de despliegue** (**público**, **compartido**, **privado o híbrido**), sus características técnicas, de calidad y de funcionamiento, y las normas técnicas que pudieran ser aplicables. Algunos de los documentos que conforman el contrato pueden resultar pertinentes para determinar su objeto (véase el párr. 38 *supra*).

Acuerdo de prestación de servicios

46. En el **acuerdo de prestación de servicios** (**SLA**) se establecen los **parámetros cuantitativos y cualitativos** que se utilizarán para evaluar la prestación de los servicios de computación en la nube, el alcance de las obligaciones contractuales y los posibles incumplimientos del proveedor. En la formulación de los **parámetros cuantitativos y cualitativos** suelen participar especialistas en tecnología de la información.

47. Por lo general, los parámetros cuantitativos se refieren a la capacidad (una determinada capacidad de almacenamiento de datos o una determinada cantidad de memoria disponible para el programa en ejecución), el **período de interrupción** o los **cortes del servicio**, la **latencia**, la **permanencia del almacenamiento de los datos**, el **período de disponibilidad del servicio**, los servicios de apoyo (por ejemplo, durante el horario de actividad del cliente o 24/7) y los planes de gestión y recuperación en casos de desastres e incidentes. En esos planes pueden establecerse parámetros como el tiempo máximo establecido para que se resuelvan los incidentes, el **tiempo de respuesta inicial** máximo, los **objetivos de punto de recuperación** y los **objetivos de tiempo de recuperación**.

48. Los parámetros cualitativos pueden referirse a la **eliminación de datos**, los **requisitos de ubicación de los datos**, la **portabilidad**, la seguridad y la privacidad o protección de los datos. Algunos aspectos del servicio pueden medirse en función tanto de parámetros cualitativos como de parámetros cuantitativos. Por ejemplo, la **elasticidad** y la **escalabilidad** pueden definirse tomando como referencia tanto la disponibilidad máxima de los recursos en un plazo mínimo establecido como la calidad y la seguridad de las medidas que pueda ser necesario adaptar según los distintos grados de confidencia-

lidad de los datos almacenados de los clientes. El cifrado puede expresarse como un valor definido de bits en reposo, en tránsito y en uso. Además de esos parámetros cuantitativos, o en lugar de ellos, se pueden utilizar parámetros cualitativos para medir el cifrado (por ejemplo, el proveedor debe asegurarse de que los datos del cliente estén cifrados cuando se transmitan por una red de comunicaciones pública, así como cuando estén en reposo en centros de datos utilizados por el proveedor).

49. Podrían pactarse distintos tipos de obligaciones (es decir, obligaciones de resultado o de medios) en función, sobre todo, de las condiciones de pago y de si se proporcionan o no **soluciones genéricas y estandarizadas para múltiples suscriptores.** El tipo de obligación que se estipule tendría consecuencias en caso de litigio, entre otras cosas con respecto a la carga de la prueba.

Evaluación de la cantidad y calidad de los servicios

50. Las partes pueden establecer en el contrato una metodología y unos procedimientos de evaluación, especificando en particular un período de referencia para la evaluación de los servicios (diario, semanal, mensual, etc.), los mecanismos de presentación de informes sobre la prestación de los servicios (es decir, la frecuencia y la forma en que se presentarán esos informes), la función y las responsabilidades de las partes, así como el sistema de medición que se utilizará (por ejemplo, si la medición se hará en el momento en que se presten los servicios o en el momento en que se utilicen). Las partes pueden convenir en que se haga una evaluación independiente de la cantidad y calidad de los servicios y pactar la forma en que se distribuirán los gastos conexos.

51. Normalmente, al cliente le interesa que la evaluación se haga en las horas de máxima intensidad de tráfico, es decir, cuando los servicios son más necesarios. Por lo general, el cliente puede realizar mediciones (o verificar las que realice el proveedor o terceros), pero solo las que evalúen la cantidad y la calidad de los servicios en el momento en que se utilicen y no cuando se presten. El cliente tal vez pueda evaluar la calidad y la cantidad de los servicios en el momento en que se prestan a partir de los informes facilitados por el proveedor o por terceros. El proveedor puede convenir en proporcionar al cliente informes sobre la cantidad y calidad de los servicios cuando este lo solicite, ya sea de 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 mediciones cuantitativas y cualitativas de los servicios. Algunos proveedores permiten que el cliente haga un seguimiento de los datos relativos a la cantidad y calidad de los servicios en tiempo real.

52. El contrato puede obligar a una de las partes o a ambas a conservar durante algún tiempo los registros correspondientes a la prestación y la utilización de los servicios. Esa información puede resultar útil a la hora de negociar modificaciones al contrato y en caso de litigio.

Política de uso aceptable

53. En la **política de uso aceptable** (**PUA**) se establecen las condiciones de uso por el cliente y sus usuarios finales de los servicios de computación en la nube comprendidos en el contrato. Su finalidad es proteger al proveedor frente a la responsabilidad que pudiera derivarse de la actividad de sus clientes y los usuarios finales de estos últimos. Se espera que los posibles clientes acepten esta política, que formará parte del contrato celebrado con el proveedor. La inmensa mayoría de las **PUA** estándar prohíben sistemáticamente determinadas actividades que los proveedores consideran que constituyen usos inadecuados o ilícitos de los **servicios de computación en la nube**. Las **PUA** pueden restringir no solo el tipo de contenido que se permite alojar en la nube, sino también el derecho del cliente a autorizar el acceso por parte de terceros (por ejemplo, nacionales de determinados países o personas incluidas en las listas de sanciones) a los datos y otros contenidos alojados en la nube. Las partes pueden convenir en eliminar algunas prohibiciones para atender necesidades empresariales concretas del cliente, siempre que esa eliminación esté permitida por la ley.

54. Es habitual que el proveedor exija, como parte de sus condiciones estándar, que los usuarios finales del cliente también respeten la **PUA** y que el cliente haga todo lo posible, o todo lo que sea razonable desde el punto de vista comercial, para garantizar que sus usuarios la respeten. Algunos proveedores pueden exigir que los clientes tomen medidas para impedir todo uso no autorizado o inadecuado por parte de terceros de los servicios de computación en la nube que se brinden con arreglo al contrato. Las partes pueden pactar un conjunto limitado de obligaciones, por ejemplo, que el cliente comunique la **PUA** a los usuarios finales conocidos, no autorice ni permita deliberadamente usos no autorizados o inadecuados, y notifique al proveedor todo uso de esa índole que llegue a su conocimiento.

55. En algunas jurisdicciones, la ley podría imponer obligaciones a los proveedores con respecto al contenido alojado en su infraestructura de computación en la nube, por ejemplo, la obligación de informar a los organismos públicos de la existencia de material ilícito. Quizás no sea posible trasladar esas obligaciones al cliente ni a los usuarios finales mediante la **PUA** ni de ninguna otra manera. Además, podrían repercutir en la privacidad y en otros aspectos y serían uno de los factores que habría que tener en cuenta al elegir un proveedor adecuado (véase la primera parte, párr. 12).

Política de seguridad

56. Mantener la seguridad del sistema y de los datos del cliente es una responsabilidad compartida de las partes. En el contrato deberían especificarse las funciones y responsabilidades que incumbirán a cada parte en lo que respecta a las medidas de seguridad, a fin de reflejar las obligaciones que correspondan a una de las partes o a ambas en virtud de normas legales imperativas.

57. Por lo general, el proveedor aplicará sus propias políticas de seguridad. En algunas situaciones, salvo en el caso de las **soluciones genéricas y estandarizadas para múltiples suscriptores**, se podría llegar a convenir en que el proveedor aplicara las políticas de seguridad del cliente. En el contrato pueden detallarse las medidas de seguridad que han de adoptarse (por ejemplo, los requisitos para la eliminación, irreversible o no, de los datos almacenados en un soporte dañado, el almacenamiento de distintos paquetes de datos en lugares diferentes o el almacenamiento de los datos del cliente en un equipo físico concreto, destinado exclusivamente a ese cliente). No obstante, incluir una cantidad excesiva de información de seguridad en el contrato puede resultar peligroso.

58. Algunas medidas de seguridad no requieren la actuación de una de las partes, sino que dependen exclusivamente de las actividades ordinarias de la otra, como las inspecciones del equipo físico en que se almacenan los datos y se ejecutan los servicios que realiza el proveedor, así como las medidas eficaces para controlar el acceso a dicho equipo. En otros casos, la actuación de una parte puede ser necesaria para que la otra pueda cumplir sus obligaciones o evaluar y vigilar la calidad de las medidas de seguridad adoptadas. Por ejemplo, es posible que el cliente tenga que actualizar las listas con las credenciales de los usuarios y sus derechos de acceso, e informar de los cambios al proveedor con la antelación suficiente para garantizar el correcto funcionamiento de los mecanismos de gestión de la identidad y de acceso. El cliente quizás tenga que comunicar también al proveedor el nivel de seguridad que deberá asignarse a cada categoría de datos.

59. Es posible que algunas amenazas a la seguridad queden fuera del marco contractual pactado entre el cliente y el proveedor, y que a raíz de ellas sea necesario ajustar las condiciones del contrato de computación en la nube a las de otros contratos suscritos por ellos (como los contratos celebrados con proveedores de servicios de Internet).

Integridad de los datos

60. En los contratos estándar de los proveedores puede figurar una cláusula de descargo general de responsabilidad en que se estipule que, en última ins-

tancia, la responsabilidad de preservar la integridad de los datos del cliente recaerá sobre este.

61. Algunos proveedores pueden estar dispuestos a asumir ciertos compromisos con respecto a la integridad de los datos (como realizar copias de seguridad con regularidad), quizás a cambio de un pago adicional. Con independencia de lo pactado con el proveedor, al cliente quizás le convendría preguntarse si no debería tener acceso a por lo menos una copia utilizable de sus datos que se encuentre fuera del control, el alcance o la influencia del proveedor y sus subcontratistas y en la que estos no participen.

Cláusula de confidencialidad

62. La decisión del proveedor de comprometerse o no a garantizar la confidencialidad de los datos del cliente dependerá de la naturaleza de los servicios que deban prestarse a este con arreglo al contrato y, en especial, de si necesitará tener acceso no cifrado a los datos para poder prestar tales servicios. Es posible que algunos proveedores no estén en condiciones de ofrecer una cláusula de confidencialidad o de no divulgación y que se eximan expresamente de asumir cualquier deber de confidencialidad respecto de los datos del cliente. Otros proveedores pueden estar dispuestos a asumir la responsabilidad de mantener la confidencialidad de los datos revelados por el cliente en el marco de la negociación del contrato, pero no la de los datos procesados durante la prestación de los servicios. Algunas cláusulas de confidencialidad estándar propuestas por los proveedores pueden no ser suficientes para garantizar el cumplimiento de la legislación aplicable.

63. En caso de que ni la ley ni el contrato impongan al proveedor un deber de confidencialidad, la responsabilidad de proteger (por ejemplo, mediante cifrado) el carácter reservado de los datos puede recaer íntegramente sobre el cliente. Cuando no sea posible negociar una cláusula general de confidencialidad aplicable a todos los datos del cliente alojados en la nube, las partes pueden pactar obligaciones de confidencialidad respecto de algunos datos de carácter delicado (estableciendo un régimen de responsabilidad independiente para el incumplimiento de la obligación de proteger la confidencialidad de dichos datos). Al cliente pueden preocuparle especialmente sus secretos comerciales, sus conocimientos especializados y la información que deba mantener en secreto por disposición de la ley o en virtud de compromisos asumidos con terceros. Las partes pueden convenir en restringir el acceso a esos datos a un número limitado de personas y exigir que cada una de ellas asuma individualmente un compromiso de confidencialidad, en especial si desempeñan funciones de alto riesgo (por ejemplo, los administradores del sistema, los auditores y las personas que se ocupan de los informes sobre la detección de

intrusos y de responder a incidentes). En esos casos, normalmente corresponderá al cliente especificar al proveedor la información confidencial, el nivel de protección necesario, las normas legales o los requisitos contractuales que sean aplicables y todos los cambios que afecten a esa información, en particular los que se produzcan en la legislación aplicable.

64. En algunos casos, puede resultar necesario revelar los datos del cliente para cumplir lo pactado en el contrato. En otros, la obligación de revelar información puede dimanar de la ley, por ejemplo, cuando en ella se establezca el deber de proporcionar información a los organismos públicos competentes (véase el párr. 82 *infra*). En tales casos estarían justificadas ciertas excepciones a las cláusulas de confidencialidad.

65. El proveedor puede a su vez imponer al cliente la obligación de no revelar información sobre las medidas de seguridad del proveedor y otros detalles de los servicios prestados al cliente de conformidad con el contrato o con la ley.

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

66. Los **datos personales** son objeto de una protección legal especial en muchas jurisdicciones. La ley aplicable al **procesamiento de datos personales** puede ser diferente de la que se aplica al contrato. En ese caso, dejará sin efecto las cláusulas contractuales que no se ajusten a ella.

67. En el contrato puede incluirse una cláusula de protección de datos o de privacidad, un acuerdo de procesamiento de datos u otro acuerdo 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 esa obligación general y que sea necesario estipular en el contrato, como mínimo, el objeto, la duración, la naturaleza y la finalidad del **procesamiento de datos personales**, el tipo de **datos personales** 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 sea posible negociar la inclusión en el contrato de una cláusula de protección de datos, al cliente tal vez le convenga revisar las condiciones estándar para determinar si le ofrecen garantías suficientes de que **los datos personales** se procesarán de acuerdo con la ley y si se prevén en ellas mecanismos de reparación adecuados en caso de daños y perjuicios.

68. Es probable que el cliente sea el **responsable de los datos** y que asuma la obligación de cumplir las leyes sobre protección de datos en lo que respecta

a los **datos personales** recopilados y procesados en la nube. Las partes pueden acordar cláusulas contractuales destinadas a garantizar el cumplimiento de la normativa aplicable en materia de protección de datos, en particular las disposiciones relativas a las solicitudes relacionadas con los **derechos de los sujetos de los datos**. También pueden estipular otras medidas específicas para el caso de que se incumplan esas cláusulas, como la posibilidad de poner fin al contrato de manera unilateral o reclamar una indemnización por daños y perjuicios.

69. En los contratos estándar de los proveedores suele estipularse que estos no asumen la función de **responsable de los datos**. Es probable que solo actúen como **procesadores de los datos** del cliente cuando los procesen siguiendo las instrucciones de este con el único fin de prestar los servicios de computación en la nube. No obstante, y con independencia de lo pactado en el contrato, es posible que en algunas jurisdicciones se considere también que el proveedor es el **responsable de los datos** cuando los procese además para sus propios fines o siguiendo instrucciones de organismos del Estado, en cuyo caso podría tener que asumir la plena responsabilidad de la protección de los **datos personales** que fueran objeto de ese **procesamiento** adicional (véase el párr. 125 *infra*).

Obligaciones derivadas de la violación de datos y otros incidentes de seguridad

70. Es posible que en la ley o el contrato, o en ambos, se establezca que cuando una de las partes se entere o tenga la sospecha de que se ha producido un **incidente de seguridad** importante para el contrato, esa parte estará obligada a notificar inmediatamente a la otra dicha circunstancia. Esa obligación puede existir además del deber general de notificación de los incidentes de seguridad que pueda estar establecido en la ley y que exija informar a todas las partes interesadas (incluidos los **sujetos de los datos**, las compañías de seguros, los organismos del Estado o el público en general) a fin de evitar o reducir al mínimo los efectos de esos incidentes.

71. Es posible que en la ley se establezcan requisitos específicos con respecto a la notificación de los incidentes de seguridad, en particular el momento en que debe realizarse esa notificación, y que se indiquen las personas responsables de que se cumplan dichos requisitos. Siempre y cuando se atengan a esas normas imperativas, las partes pueden especificar en el contrato el plazo en que deberá realizarse la notificación (por ejemplo, un día después de que la parte haya tenido conocimiento del incidente o la amenaza), así como la forma y el contenido que esta deberá tener. En cuanto al contenido de la notificación, generalmente abarca las circunstancias y la causa del incidente, el tipo de datos afectados, las medidas que se prevé adoptar para resolver el incidente, el plazo en que se espera resolverlo y los planes de emergencia que se han de

emplear mientras se resuelve. También puede incluirse en la notificación información sobre intentos fallidos de quebrantar la seguridad, ataques contra objetivos concretos (desglosados por usuario del cliente, aplicación específica o máquina física concreta), tendencias y estadísticas. Al establecer los requisitos de notificación se suele tener en cuenta la necesidad de no revelar información delicada que pueda poner en peligro los sistemas, la red o las operaciones de la parte afectada.

72. La ley o el contrato pueden exigir que el proveedor, el cliente o ambos, por sí mismos o con la participación de un tercero, adopten medidas después de un incidente de seguridad (denominadas "medidas posteriores al incidente"), entre ellas el aislamiento o la puesta en cuarentena de las zonas afectadas, la realización de análisis de las causas profundas del incidente y la elaboración de un informe de análisis del incidente. Este informe puede ser realizado por la parte afectada, o por esta junto con la otra parte, o por un tercero independiente. Las medidas posteriores al incidente pueden variar en función de las categorías de datos almacenados en la nube y otros factores.

73. Un incidente de seguridad grave que tuviera como consecuencia, por ejemplo, la pérdida de datos podría dar lugar a la resolución del contrato.

Requisitos de ubicación de los datos

74. En sus condiciones estándar, el proveedor puede reservarse expresamente el derecho de alojar los datos del cliente en cualquier país en que operen él o sus subcontratistas. Es muy probable que se siga dicha práctica incluso cuando no se haya establecido expresamente ese derecho en el contrato, ya que en la prestación de los **servicios de computación en la nube** está implícito el hecho de que, por regla general, esos servicios se suministran desde más de un lugar (por ejemplo, las copias de seguridad y la protección antivirus pueden hacerse a distancia y el servicio de apoyo al cliente puede ofrecerse siguiendo el modelo de **aprovechamiento de los husos horarios**). Es posible que esa práctica no se ajuste a los **requisitos de ubicación de los datos** aplicables a una de las partes o a ambas (véase la primera parte, párrs. 10 y 11).

75. En el contrato pueden incluirse medidas de salvaguardia destinadas a garantizar el cumplimiento de los **requisitos de ubicación de los datos**, como la prohibición de trasladar datos y otros contenidos fuera del lugar especificado o la obligación de obtener una autorización previa de la otra parte para hacerlo. Por ejemplo, se puede incluir un parámetro cualitativo en un **SLA** para garantizar que los datos del cliente (incluidas todas sus copias, **metadatos** y copias de seguridad) se almacenen exclusivamente en centros de datos ubicados físicamente en las jurisdicciones indicadas en el contrato y cuya pro-

piedad y administración correspondan a entidades establecidas en dichas jurisdicciones. Como alternativa a lo anterior, se podría utilizar ese parámetro, por ejemplo, para prohibir que los datos se trasladaran fuera de un país o región en particular y a la vez permitir que se duplicaran en un país determinado o en cualquier otro lugar, salvo en un país en concreto.

D. DERECHOS EN RELACIÓN CON LOS DATOS Y OTROS CONTENIDOS DEL CLIENTE

Derechos del proveedor en relación con los datos del cliente a efectos de la prestación de los servicios

76. Los proveedores suelen reservarse el derecho de acceder a los datos del cliente siempre y cuando "necesiten conocerlos". Normalmente, esto permite que los empleados del proveedor, los subcontratistas y otros terceros (por ejemplo, los auditores) tengan acceso a los datos del cliente cuando sea necesario para prestar los servicios de computación en la nube (con fines de mantenimiento, apoyo y seguridad, entre otros) y supervisar el cumplimiento de lo establecido en la **PUA**, las **licencias de PI**, el **SLA** y otros documentos contractuales. Las partes pueden pactar en qué casos se permitirá el acceso del proveedor a los datos del cliente y qué medidas se adoptarán para garantizar la confidencialidad y la integridad de dichos datos.

77. Puede considerarse que, cuando el cliente solicita al proveedor un determinado servicio o funcionalidad, 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 está obligado a realizar periódicamente copias de seguridad de los datos del cliente, deberá tener derecho a hacer copias de los datos para poder llevar a cabo esa tarea. Del mismo modo, si los subcontratistas han de manipular los datos del cliente, el proveedor debe tener la posibilidad de transferírselos.

78. En el contrato puede indicarse expresamente cuáles son los derechos relacionados con los datos que el cliente otorga al proveedor y que son necesarios para el cumplimiento del contrato; si el proveedor está autorizado a ceder esos derechos a terceros (por ejemplo, a sus subcontratistas) y, si lo estuviera, en qué medida puede hacerlo; y a qué espacio geográfico y de tiempo se circunscriben los derechos concedidos expresa o implícitamente. Las limitaciones geográficas pueden ser especialmente importantes cuando la ley prohíbe que los datos salgan de un determinado país o región (véase la primera parte, párrs. 10 y 11). En los contratos suele indicarse si el cliente tiene la facultad de revocar los derechos otorgados expresa o implícitamente y, si así fuera, en

qué condiciones puede hacerlo. Dado que la capacidad de prestar los servicios con el nivel de calidad exigido puede depender de los derechos que otorgue el cliente, la revocación de algunos de ellos podría tener como consecuencia directa la modificación o resolución del contrato.

Utilización por el proveedor de los datos del cliente con otros fines

79. En la mayoría de las jurisdicciones no se concede automáticamente al proveedor el derecho a utilizar los datos del cliente para sus propios fines. El proveedor puede solicitar permiso para utilizar los datos del cliente con fines distintos de los relacionados con la prestación de los servicios de computación en la nube previstos en el contrato (por ejemplo, con fines publicitarios o para generar estadísticas, elaborar informes analíticos o de predicciones, participar en otras prácticas de extracción de datos, etc.). En ese contexto, cabría plantearse las preguntas siguientes, entre otras: *a)* qué información se recopilará sobre el cliente y sus usuarios finales y por qué motivos, y con qué fines la recopilará y utilizará el proveedor; *b)* si esa información se va a comunicar a otras organizaciones, empresas o particulares y, de ser así, por qué razón se comunicará y si ello se hará con el consentimiento del cliente o sin él; y *c)* de qué manera se va a garantizar el cumplimiento de las políticas de confidencialidad y seguridad si el proveedor transmite esa información con terceros. Cuando el uso que hace el proveedor de los datos del cliente afecta a **datos personales**, lo más probable es que las partes evalúen cuidadosamente sus respectivas obligaciones de cumplir lo dispuesto en las leyes aplicables en materia de protección de datos.

80. En los contratos en que se otorga al proveedor el derecho a utilizar los datos del cliente para sus propios fines, es posible que también se enumeren los motivos por los que se permitirá dicho uso, se establezca la obligación de anonimizar los datos del cliente y ocultar su identidad a fin de garantizar el cumplimiento de la normativa aplicable en materia de protección de datos y otras normas, y se impongan límites a la reproducción del contenido y a su comunicación al público. Es una práctica común permitir que el proveedor utilice los datos del cliente para sus propios fines durante el plazo de vigencia del contrato o tras su extinción, pero solo en forma de datos abiertos anonimizados o como información agregada que no revele la identidad del cliente.

Utilización por el proveedor del nombre, el logotipo y la marca del cliente

81. En las condiciones estándar de los proveedores es posible que se conceda a estos el derecho a utilizar en su propia publicidad los nombres, logotipos y

marcas del cliente. Las partes pueden convenir en suprimir o modificar esas disposiciones, por ejemplo, limitando el uso que se puede hacer del nombre del cliente y exigiendo que se obtenga la autorización previa de este para poder utilizar su nombre, logotipo y marca.

Medidas adoptadas por el proveedor con respecto a los datos del cliente en cumplimiento de una orden del Estado o de la normativa vigente

82. En sus condiciones estándar, el proveedor puede reservarse la facultad discrecional de revelar los datos del cliente o dar acceso a dichos datos a organismos públicos (incluyendo, por ejemplo, una mención como la siguiente: "cuando hacerlo sea en el interés superior del proveedor"). En las condiciones estándar del proveedor también se suele otorgar a este el derecho a retirar o bloquear los datos del cliente inmediatamente después de que tome conocimiento o se entere de la existencia de contenido ilícito en dichos datos, o cuando tenga que hacer respetar el **derecho al olvido de los sujetos de los datos**, a fin de no incurrir en responsabilidad legal (con arreglo al procedimiento de "notificación y retirada" (véase el párr. 128 *infra*)). Las partes pueden convenir en restringir los casos en que el proveedor podrá actuar de ese modo, por ejemplo, cuando un tribunal u otro órgano del Estado le ordene facilitar el acceso a los datos, suprimirlos o modificarlos.

83. Las partes pueden acordar, como mínimo, que se notifiquen sin demora al cliente las órdenes del Estado o las propias decisiones del proveedor con respecto a los datos del cliente, y que se incluya en la notificación una descripción de los datos de que se trate, a menos que dicha notificación sea contraria a la ley. Cuando no sea posible realizar la notificación ni dar intervención al cliente por adelantado, se puede establecer en el contrato la obligación de que el proveedor notifique esa misma información al cliente inmediatamente después. Las partes también pueden convenir en incluir cláusulas que obliguen a llevar un registro de todas las órdenes, solicitudes y demás actividades relacionadas con los datos del cliente, y a conceder a este último acceso a ese registro.

Derechos en relación con los datos obtenidos de los servicios de nube

84. Las partes pueden estipular los derechos que tendrá el cliente en relación con los **datos obtenidos de los servicios de nube** y la forma en que podrán ejercerse esos derechos durante el período de vigencia de la relación contractual y tras la extinción del contrato.

Cláusula de protección de los derechos de PI

85. Algunos tipos de contratos de computación en la nube pueden dar origen a objetos de derechos de PI, ya sea como resultado de la acción conjunta del proveedor y el cliente (por ejemplo, mejoras en los servicios derivadas de sugerencias del cliente) o solo del cliente (nuevas aplicaciones, programas informáticos y otras obras originales). En el contrato puede incluirse una cláusula expresa sobre PI que determine a cuál de las partes en el contrato pertenecen los derechos de PI sobre diversos objetos desplegados o desarrollados en la nube, y cómo pueden las partes ejercer esos derechos. Cuando no exista la posibilidad de negociar este aspecto, el cliente tal vez desee revisar las cláusulas de PI a fin de determinar si el proveedor le ofrece garantías suficientes y pone a su disposición los mecanismos necesarios para proteger y ejercer sus derechos de PI y evitar los riesgos de **dependencia** (véase la primera parte, párrs. 23 a 26).

Interoperabilidad y portabilidad

86. Es posible que no exista ninguna obligación legal de garantizar la **interoperabilidad** y la **portabilidad**. La carga de crear procedimientos compatibles de exportación de datos puede recaer íntegramente sobre el cliente a menos que en el contrato se prevea otra cosa, por ejemplo, que se asuman obligaciones con respecto a la interoperabilidad y la portabilidad y que se preste asistencia para exportar los datos en el momento en que se extinga el contrato (véase el párr. 161 *infra*). En el contrato se puede exigir que, para la exportación de datos y otros contenidos, se utilicen formatos interoperables o estandarizados que sean comunes y ampliamente utilizados, o permitir que se elija entre los formatos de exportación disponibles. También pueden incluirse en el contrato cláusulas que regulen los derechos relativos a los productos y aplicaciones o programas informáticos de propiedad conjunta, sin los cuales podría resultar imposible utilizar los datos y demás contenidos en otro sistema (véase el párr. 85 *supra*).

Recuperación de datos con una finalidad jurídica

87. Es posible que los clientes necesiten buscar y encontrar datos alojados en la nube en su forma original para cumplir determinadas obligaciones legales (por ejemplo, en el marco de una investigación), y que los registros electrónicos tengan que ajustarse a las normas de auditoría y los requisitos exigidos en materia de prueba. Algunos proveedores quizás estén en condiciones de prestar asistencia a los clientes para recuperar los datos en el formato exigido por la ley. En el contrato puede establecerse la forma y las condiciones en que se prestará dicha asistencia.

Eliminación de datos

88. La **eliminación de datos** es una cuestión que puede plantearse durante todo el período de vigencia del contrato, aunque muy especialmente en el momento de su extinción (véase el párr. 162 *infra*). Por ejemplo, es posible que determinados datos deban eliminarse siguiendo el plan de conservación del cliente. Puede ser necesario destruir datos de carácter delicado 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 en que se almacenaron dichos datos). También puede ser necesario eliminar datos a solicitud de un organismo encargado de hacer cumplir la ley o cuando se confirme que se han vulnerado derechos de PI (véase el párr. 82 *supra*).

89. Es posible que en las condiciones estándar del proveedor se establezca únicamente que los datos del cliente se eliminarán cada cierto tiempo. Las partes pueden convenir en que los datos, sus copias de seguridad y los **metadatos** se eliminen de manera inmediata, eficaz, irrevocable y permanente, de conformidad con el calendario de conservación y eliminación de datos u otras autorizaciones o solicitudes que el cliente comunique al proveedor. En el contrato se puede establecer el plazo y otras condiciones relativas a la eliminación de datos, como la obligación de confirmar la eliminación una vez realizada y facilitar el acceso a los registros de auditoría de las actividades de eliminación de datos.

90. También es posible que, en función de la naturaleza y el grado de confidencialidad de los datos, se convenga en aplicar determinadas normas o técnicas de eliminación. Quizás se exija al proveedor que elimine los datos almacenados en distintos lugares y soportes, entre ellos los sistemas de los subcontratistas y otros terceros, y que la eliminación se haga en diverso grado, desde una supresión de los datos que asegure su confidencialidad, hasta su completa eliminación o la destrucción del equipo físico en que están almacenados. Los procedimientos de eliminación que conllevan la destrucción del equipo en lugar de su redistribución son más seguros, pero pueden resultar más costosos y no siempre es posible llevarlos a cabo (por ejemplo, cuando existen datos de otras personas almacenados en el mismo equipo físico). Estos aspectos pueden dar lugar a que se pacte en el contrato la obligación de utilizar una infraestructura aislada para almacenar los datos especialmente delicados del cliente.

E. AUDITORÍAS Y SUPERVISIÓN

Actividades de supervisión

91. Es posible que las partes necesiten supervisar mutuamente sus actividades para asegurarse de que se cumpla lo estipulado en el contrato y se respete la normativa aplicable (por ejemplo, que el cliente y sus usuarios finales respeten la **PUA** y las **licencias de PI** y que el proveedor actúe de conformidad con el **SLA** y la política de protección de datos). Algunas actividades de supervisión, como las relacionadas con el **procesamiento de datos personales**, pueden ser obligatorias por disposición de la ley.

92. Es posible que en el contrato se especifiquen las actividades de supervisión periódicas o recurrentes que se llevarán a cabo y la parte que se encargará de su ejecución, imponiéndose a la otra parte la obligación de facilitar dicha supervisión. Quizás en el contrato también se prevea la posibilidad de realizar actividades de supervisión con carácter excepcional y se contemplen diversas formas de llevarlas a cabo. En el contrato se puede establecer asimismo el deber de notificar a la otra parte y las obligaciones de confidencialidad que se asumirán en relación con esas actividades de supervisión.

93. Una supervisión excesiva puede afectar a la cantidad o la calidad de los servicios y aumentar el costo de estos. En el contrato se puede pactar la obligación de suspender la supervisión en determinados casos, por ejemplo, cuando esta tenga efectos negativos graves en la cantidad o la calidad de los servicios. Esta preocupación puede plantearse principalmente en el caso de los servicios que deben prestarse casi en tiempo real.

Auditorías y pruebas de seguridad

94. Es común que se practiquen auditorías y pruebas de seguridad, especialmente para comprobar la eficacia de las medidas de seguridad. En algunos casos deben realizarse por disposición de la ley. El contrato puede contener cláusulas en las que se definan los derechos de ambas partes en materia de auditoría y se establezca el alcance, la frecuencia, las formalidades y el costo de las auditorías. También es posible que el contrato imponga a las partes la obligación de comunicarse mutuamente los resultados de las auditorías o las pruebas de seguridad encargadas por cada una de ellas. Los derechos contractuales o las obligaciones legales de una parte en materia de auditorías y pruebas de seguridad pueden complementarse en el contrato, imponiendo a la otra parte la correspondiente obligación de facilitar el ejercicio de esos derechos o el cumplimiento de esas obligaciones (por ejemplo, permitiéndole que acceda a los centros de datos pertinentes).

95. Las partes pueden convenir en que las auditorías o las pruebas de seguridad solo sean realizadas por organizaciones profesionales, o en que el proveedor o el cliente puedan optar por encomendar la tarea a una organización profesional. En el contrato se pueden especificar los requisitos que deben reunir esos terceros y las condiciones exigidas para su participación, en particular en lo que respecta a la distribución de los gastos. Las partes pueden estipular medidas especiales para que se realicen auditorías o pruebas de seguridad cada vez que se produzca un incidente, dependiendo de la gravedad y la naturaleza de este (por ejemplo, puede obligarse a la parte responsable del incidente a reembolsar la totalidad o parte de los gastos).

F. CONDICIONES DE PAGO

Pago por uso

96. Dado que el precio es un elemento esencial del contrato, puede resultar imposible obtener la ejecución de un contrato en el que se haya omitido el precio o un mecanismo que permita determinarlo.

97. Una característica de los servicios de computación en la nube es la de ser **autoservicios a pedido**, por lo que su sistema de facturación suele ser del tipo **"pago por uso"** (*pay-as-you-go*). Es habitual que en el contrato se especifique el precio unitario correspondiente al volumen acordado de los servicios de computación en la nube que se prestarán (por ejemplo, el precio correspondiente al número de usuarios, al número de usos o al tiempo de utilización especificados). Se pueden establecer escalas de precios u otros ajustes en el precio, en particular descuentos por volumen, como incentivos o sanciones para cualquiera de las partes. También es común que se ofrezcan servicios a título gratuito durante un período de prueba, o que no se cobre por algunos servicios. Aunque puede haber muchas variaciones en el cálculo del precio, la inclusión de una cláusula de precio clara y transparente que ambas partes entiendan puede evitar conflictos y pleitos en el futuro.

Derechos de licencia

98. Es posible que las partes deseen aclarar en el contrato si el importe que se pagará por los servicios de computación en la nube incluye los derechos 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.

99. Los derechos de licencia pueden calcularse sobre la base del número de usuarios o el número de instancias 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, a diferencia de los no profesionales). Las distintas estructuras de pago pueden tener consecuencias diferentes. Por ejemplo, el costo de la licencia de un programa informático para el cliente puede aumentar de manera exponencial si cada vez que se conecte una nueva máquina a ese programa se cobra una instancia, aun cuando el cliente esté utilizando el mismo número de instancias durante el mismo período.

100. El contrato puede establecer el número total de usuarios que podrán utilizar un programa informático amparado por el acuerdo de licencia, el número de usuarios pertenecientes a cada categoría (por ejemplo, empleados, contratistas independientes y proveedores) y los derechos que se concederán a cada una de esas categorías. También pueden indicarse en el contrato los derechos de acceso y uso que estarán comprendidos en la licencia, así como los casos de acceso y uso por parte del cliente y sus usuarios finales que podrán dar lugar a que se amplíe el alcance de la licencia y a que, por consiguiente, se eleve el importe de los derechos que deberán pagarse por ella.

Costos adicionales

101. El precio puede abarcar también algunos costos puntuales (por ejemplo, los costos de configuración y migración a la nube; véase la primera parte, párrs. 32 y 33). Asimismo, es posible que el proveedor ofrezca otros servicios adicionales a cambio de un pago aparte (por ejemplo, servicios de apoyo al cliente fuera del horario comercial, que se cobran por tiempo de utilización o se prestan a cambio de un precio fijo).

102. En algunas jurisdicciones, los servicios de computación en la nube pueden estar comprendidos en la categoría de servicios o bienes imponibles. Las partes tal vez deseen prever en el contrato los efectos de los impuestos en las condiciones de pago.

Otras condiciones de pago

103. Las condiciones de pago pueden abarcar las modalidades de facturación (por ejemplo, la facturación electrónica) y la forma y el contenido de las facturas, aspecto que puede resultar importante a los efectos del cumplimiento de las normas tributarias. Es posible que los organismos tributarios de algunas jurisdicciones no acepten facturas electrónicas (aunque esto es cada vez menos frecuente debido a la disminución del uso del papel) o exijan que se utilice

un formato especial, por ejemplo, uno que obligue a detallar por separado los impuestos aplicables a los servicios de computación en la nube.

104. Las partes tal vez deseen incluir en el contrato, entre las condiciones de pago, las fechas de vencimiento, la moneda, el tipo de cambio aplicable, la forma de pago, las sanciones por mora y los procedimientos de solución de las controversias que se planteen en relación con los pagos.

G. CAMBIOS EN LOS SERVICIOS

105. Los **servicios de computación en la nube** son, por naturaleza, flexibles y fluctuantes. La **elasticidad,** la **escalabilidad** y el **autoservicio a pedido** que caracterizan a los **servicios de computación en la nube** suelen ofrecerse introduciendo en el contrato múltiples opciones que el cliente puede utilizar para adaptar el consumo de los servicios a sus necesidades. Con ello se logra que no sea necesario volver a negociar el contrato cada vez que el cliente desee cambiar el consumo de los servicios.

106. Por su parte, el proveedor puede reservarse el derecho a modificar su cartera de servicios a su entera discreción. Quizás sea conveniente tratar esas modificaciones de manera distinta en el contrato, dependiendo de si los cambios se refieren a los servicios principales o a los servicios auxiliares y cuestiones de apoyo. Quizás también corresponda dar a las modificaciones que pudieran afectar negativamente a los servicios un tratamiento contractual diferente al previsto para las modificaciones que supongan mejoras (por ejemplo, la sustitución de una oferta estándar de servicios de computación en la nube por otra mejorada, con mayores niveles de seguridad o menores tiempos de respuesta). Algunos cambios realizados unilateralmente por el proveedor en las condiciones estipuladas en el contrato pueden tener graves consecuencias para el cliente, especialmente cuando el cambio implica tener que incurrir en gastos elevados de migración a otro sistema.

Cambios en el precio

107. El proveedor puede reservarse el derecho a modificar unilateralmente el precio o las escalas de precios de sus servicios. Las partes pueden convenir en especificar en el contrato la metodología de fijación del precio (por ejemplo, con qué frecuencia y en qué medida el proveedor puede aumentar los precios). Se puede fijar un límite máximo a los precios, que se calculará de acuerdo con un determinado índice de precios al consumo, un porcentaje fijo o el listado de precios del proveedor vigente en un momento dado. En el

contrato se puede establecer la obligación de notificar con antelación todo aumento del precio y detallar las consecuencias de que el cliente no acepte ese aumento.

Actualizaciones

108. Si bien es posible que las actualizaciones sean en interés del cliente, también pueden causar trastornos en lo que respecta a la disponibilidad de los **servicios de computación en la nube**, ya que pueden conllevar **períodos de interrupción** relativamente prolongados durante el horario normal de funcionamiento, aun cuando se trate de servicios prestados de forma ininterrumpida. Las partes pueden convenir en que se notifique al cliente con antelación las actualizaciones pendientes y sus consecuencias, y en que, como norma general, estas se lleven a cabo durante los períodos en que el cliente tenga poca demanda o ninguna. También pueden establecerse en el contrato los procedimientos que deberán emplearse para comunicar y resolver los eventuales problemas que surjan.

109. Es posible que las actualizaciones tengan otros efectos negativos, como la necesidad de introducir cambios en las aplicaciones o los sistemas informáticos del cliente o de capacitar nuevamente a los usuarios de este. En el contrato puede preverse la forma de distribuir los gastos derivados de las actualizaciones. Las partes pueden acordar asimismo que, cuando se vayan a realizar cambios importantes en la versión anterior, esta se mantenga en paralelo con la nueva versión durante un período convenido, a fin de garantizar la continuidad de las operaciones del cliente. También es posible prever en el contrato la asistencia que puede ofrecer el proveedor en relación con los cambios que se introduzcan en las aplicaciones o los sistemas informáticos del cliente y la nueva capacitación que en su caso sea necesario impartir a los usuarios finales del cliente.

Degradación o interrupción de los servicios

110. Los avances tecnológicos, la presión de la competencia y otras circunstancias pueden llegar a provocar la degradación o la interrupción de algunos servicios de computación en la nube, que podrán ser sustituidos o no por otros servicios. El proveedor puede reservarse en el contrato el derecho a modificar su oferta de servicios (por ejemplo, cancelando una parte de ellos). Sin embargo, incluso la interrupción de solo algunos servicios de computación en la nube por parte del proveedor puede hacer que el cliente incurra en responsabilidad frente a sus usuarios finales.

111. En el contrato se puede establecer la obligación de notificar de antemano los cambios al cliente, el derecho de este último a poner fin al contrato si los cambios fueran inaceptables, y un período de conservación suficiente para garantizar la oportuna **reversibilidad** de los datos u otros contenidos del cliente que hubiesen resultado afectados. En algunos contratos se prohíbe hacer modificaciones que puedan tener efectos negativos en la naturaleza, el alcance o la calidad de los servicios prestados, o solo se permite hacer "modificaciones razonables desde el punto de vista comercial".

Notificación de los cambios

112. En las condiciones estándar de los proveedores puede estar prevista la obligación de estos de notificar al cliente los cambios en las condiciones de los servicios. Si no lo está, es posible que se pida a los clientes que comprueben periódicamente si se han introducido cambios en el contrato. Los documentos que integran el contrato pueden ser numerosos (véase el párr. 38 *supra*). Es posible que algunos de ellos incorporen por remisión condiciones y políticas establecidas en otros documentos, los que a su vez quizás incorporen por remisión otras condiciones y políticas, y todas ellas pueden ser modificadas unilateralmente por el proveedor. Esos distintos documentos no tienen que estar alojados necesariamente en un único lugar del sitio web del proveedor. Por lo tanto, quizás no sea fácil detectar los cambios introducidos por el proveedor en el contrato.

113. Dado que la utilización continuada de los servicios por parte del cliente se considera una aceptación de las modificaciones realizadas en las condiciones de los servicios, las partes pueden convenir en que todo cambio que se prevea introducir en esas condiciones se notifique al cliente con suficiente antelación a la fecha de su entrada en vigor. Asimismo, las partes pueden acordar que el cliente tenga acceso a los registros de auditoría relativos a la evolución de los servicios y que se mantengan todas las condiciones pactadas y las definiciones de los servicios correspondientes a una determinada versión o edición.

H. SUSPENSIÓN DE LOS SERVICIOS

114. En las condiciones estándar de los proveedores puede establecerse el derecho de estos a suspender los servicios a su entera discreción en cualquier momento. Uno de los motivos que se aducen comúnmente para justificar la suspensión unilateral de los servicios por el proveedor es el acaecimiento de "hechos imprevisibles". Estos suelen definirse de manera amplia, como todo impedimento ajeno a la voluntad del proveedor, incluido el incumplimiento de los subcontratistas, los proveedores del proveedor y otros terceros que parti-

cipen en la prestación de los servicios de computación en la nube al cliente, como los proveedores de acceso a Internet.

115. Las partes pueden convenir en que solo se permita suspender los servicios en unos pocos casos definidos en el contrato (por ejemplo, cuando el cliente incurra en un incumplimiento esencial del contrato, como la falta de pago). El derecho a suspender los servicios debido a hechos imprevisibles puede estar sometido a la condición de que se ponga debidamente en marcha un plan de continuidad de las operaciones y recuperación en casos de desastre. El contrato puede exigir que se incluyan en ese plan medidas de protección frente a los peligros más comunes a que está expuesta la prestación de servicios de computación en la nube y que el plan se someta a la consideración y aprobación de la otra parte. Algunas de esas medidas de protección podrían consistir en disponer de un sitio de recuperación en casos de desastre ubicado en otro lugar geográfico que permita una transición imperceptible, y en utilizar sistemas de suministro ininterrumpido de energía y generadores de apoyo.

I. SUBCONTRATISTAS, PROVEEDORES DEL PROVEEDOR Y EXTERNALIZACIÓN

Identificación de los participantes en la cadena de subcontratación

116. La subcontratación, los **servicios estratificados de computación en la nube** y la externalización son prácticas habituales en el entorno de la computación en la nube. En las condiciones estándar de los proveedores, estos pueden reservarse expresamente el derecho a prestar los servicios de computación en la nube al cliente por conducto de terceros, o ese derecho puede estar implícito debido a la propia naturaleza de los servicios que han de prestarse. Al proveedor quizás le interese conservar la mayor flexibilidad posible en ese sentido.

117. Las partes pueden estar obligadas por ley a especificar en el contrato los terceros que participarán en la prestación de los servicios de computación en la nube. La identificación de esos terceros también puede ser útil para el cliente a los efectos de verificar cierta información, especialmente porque le permite determinar si esos terceros cumplen los requisitos de seguridad, confidencialidad, protección de datos y otros requisitos establecidos en el contrato o en la ley, y comprobar la inexistencia de conflictos de intereses respecto de esos terceros.

118. Esa información puede utilizarse también para mitigar el riesgo de incumplimiento del contrato por el proveedor debido al incumplimiento de terceros. Por ejemplo, el cliente puede optar por contratar directamente con los

terceros que resultan imprescindibles para la ejecución del contrato de computación en la nube, sobre todo en lo relativo a cuestiones tan delicadas como la confidencialidad y el **procesamiento de datos personales**. El cliente también puede tratar de negociar con los terceros más importantes para que estos asuman la obligación de intervenir si el proveedor no cumple lo establecido en el contrato, en particular si incurre en insolvencia.

119. Es posible que el proveedor no esté en condiciones de identificar a todos los terceros involucrados, aunque quizás sí a los que desempeñan funciones de importancia clave. La composición del conjunto de terceros que intervienen en la prestación de los servicios de computación en la nube puede variar durante el período de vigencia del contrato (véanse los párrs. 120 y 121 *infra*).

Cambios en la cadena de subcontratación

120. Es habitual que se produzcan cambios unilaterales en la cadena de subcontratación. En el contrato puede especificarse si se permite hacer cambios en la cadena de subcontratación y, de ser así, en qué condiciones pueden realizarse esos cambios (por ejemplo, el cliente puede reservarse el derecho a investigar los antecedentes de cualquier tercero que se prevea incorporar a la prestación de los servicios de computación en la nube y vetarlo antes de que se realice el cambio). Como alternativa a lo anterior, se podría incluir en el contrato una lista de terceros aprobados previamente por el cliente, entre los que el proveedor podrá elegir cuando sea necesario. Otra posibilidad sería que el cambio quedara supeditado a la posterior aprobación del cliente y que, si este no aceptase el cambio, los servicios siguieran prestándose con la participación del tercero anterior o con otro tercero aprobado previamente o que las partes designaran de común acuerdo. De lo contrario, se podría poner fin al contrato.

121. Las disposiciones imperativas de la ley aplicable pueden establecer las circunstancias en que los cambios introducidos en la cadena de subcontratación del proveedor podrían hacer necesario resolver el contrato.

Armonización de las condiciones del contrato con las de otros contratos vinculados

122. Las partes pueden tener la obligación legal o contractual de ajustar las condiciones del contrato a las de otros contratos vigentes o futuros vinculados al primero, a fin de asegurar la confidencialidad y el cumplimiento de los requisitos en materia de protección y **ubicación de los datos**. En el contrato puede establecerse la obligación de cada parte de proporcionar a la otra, con fines de verificación, copias de los contratos vinculados.

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

123. Si bien en el contrato de computación en la nube se puede incluir una lista de los terceros que sean imprescindibles para su ejecución, esos terceros no serán partes en el contrato celebrado entre el cliente y el proveedor y solo responderán de las obligaciones que hayan contraído en virtud de sus contratos con el proveedor. La constitución, en beneficio del cliente, de derechos de terceros beneficiarios en los contratos vinculados, o la incorporación del cliente como parte en dichos contratos vinculados, permitiría al cliente recurrir directamente contra el tercero en caso de que este incurriera en incumplimiento del contrato vinculado.

124. Con arreglo a lo dispuesto en la ley aplicable o en el contrato, el proveedor puede tener que responder frente al cliente de cualquier cuestión encomendada a un tercero a quien el proveedor haya hecho participar en la ejecución del contrato. La ley puede establecer, en particular, la responsabilidad solidaria del proveedor y sus subcontratistas respecto de las cuestiones que se planteen en relación con el **procesamiento de datos personales**, según el grado de participación que hayan tenido los subcontratistas en el procesamiento de esos datos.

J. RESPONSABILIDAD

Restricciones legales a la libertad contractual

125. Si bien en la mayoría de los ordenamientos jurídicos se reconoce generalmente el derecho de las partes contratantes a distribuir los riesgos y la responsabilidad y a limitar o excluir su responsabilidad mediante la inclusión de cláusulas a esos efectos en el contrato, ese derecho suele estar sujeto a ciertos límites y condiciones. Por ejemplo, un factor importante que influye en la distribución de los riesgos y la responsabilidad en lo que respecta al **procesamiento de datos personales** es la función que asume cada parte en relación con los **datos personales** alojados en la nube. En algunas jurisdicciones, la ley aplicable en materia de protección de datos impone una responsabilidad mayor al **responsable de los datos personales** que a los **procesadores** de esos datos. Aunque en el contrato se estipule otra cosa, el manejo efectivo de esos datos será lo que normalmente determine el régimen jurídico al que estará sometida una parte con arreglo a la ley aplicable. Los **sujetos de los datos** que hayan sufrido pérdidas como consecuencia del procesamiento ilegal de **datos personales** o de cualquier acto incompatible con las normas nacionales de protección de datos pueden tener derecho a reclamar una indemnización directamente al **responsable de los datos**.

126. Además, en muchas jurisdicciones la exención total de la responsabilidad personal derivada de la propia culpa no es admisible o bien está sujeta a ciertos límites. Tal vez no sea posible excluir íntegramente la responsabilidad por lesiones personales (incluidas la enfermedad y la muerte) y por negligencia grave, dolo, vicios, incumplimiento de las obligaciones básicas y esenciales para la ejecución del contrato o incumplimiento de los requisitos reglamentarios aplicables. Algunos tipos de cláusulas de limitación de la responsabilidad, como las que eximen de responsabilidad al proveedor por **incidentes de seguridad** en los casos en que el cliente no tiene el control de las medidas de seguridad ni la capacidad de adoptarlas, pueden considerarse "abusivas" y, por ende, nulas. Las condiciones de los contratos de adhesión, que normalmente no se negocian sino que vienen preestablecidas por una de las partes, pueden tener que someterse a un examen particularmente minucioso. Además, la ley puede prever la responsabilidad ilimitada por determinados tipos de vicios (por ejemplo, defectos en los equipos físicos o los programas informáticos).

127. Las instituciones públicas pueden tener limitaciones legales para asumir determinadas responsabilidades, o la obligación de obtener la autorización previa de un órgano estatal competente para hacerlo. También les puede estar prohibido aceptar que se excluya o limite la responsabilidad de un proveedor con carácter general o por las acciones u omisiones definidas en la ley.

128. Por otra parte, la ley aplicable puede permitir que se exima de responsabilidad a una de las partes si esta cumple determinados requisitos que, de no satisfacerse, la expondrían al riesgo de incurrir en responsabilidad. Por ejemplo, según el procedimiento de "notificación y retirada" (véase el párr. 82 *supra*) vigente en algunas jurisdicciones, el proveedor queda liberado de responsabilidad por alojar contenido ilícito en su infraestructura de nube si lo retira en cuanto se entere de su existencia.

129. En algunas jurisdicciones es necesario incluir en el contrato las cláusulas de descargo y limitación de la responsabilidad acordadas por las partes para que sean exigibles. La ley aplicable podría supeditar la validez y eficacia de esas cláusulas al cumplimiento de determinados requisitos de forma o de otra índole.

Otras cuestiones que deben tenerse en cuenta al redactar cláusulas de responsabilidad

130. Al negociar la distribución de los riesgos y la responsabilidad, normalmente se tendrán en cuenta el importe cobrado, en su caso, por los servicios de computación en la nube, así como los riesgos inherentes a la prestación de esos servicios. Aunque las partes tienden por lo general a excluir o limitar la

responsabilidad derivada de factores ajenos a su voluntad o que solo pueden controlar hasta cierto punto (como el comportamiento de los usuarios finales o las acciones u omisiones de los subcontratistas), el grado de control no siempre será un factor decisivo. Una parte puede estar dispuesta a asumir riesgos y responsabilidad por elementos ajenos a su voluntad con el fin de distinguirse en el mercado. No obstante, es más probable que los riesgos y la responsabilidad de esa parte aumenten progresivamente de forma proporcional a los elementos que estén bajo su control.

131. Por ejemplo, en los servicios de tipo **SaaS** en que se utilizan programas informáticos de oficina de carácter estándar, es probable que el proveedor sea responsable de prácticamente todos los recursos proporcionados al cliente, por lo que podría incurrir en responsabilidad en todos los casos en que esos recursos no estuviesen disponibles o no funcionaran correctamente. No obstante, incluso en esos 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 hecho de no realizar las copias de seguridad necesarias podría acarrear la pérdida del derecho a reclamar contra el proveedor en caso de pérdida de los datos. En cambio, en el caso de los servicios de tipo **IaaS** y **PaaS**, el proveedor podría tener que responder únicamente de la infraestructura o las plataformas proporcionadas (como los equipos físicos, el sistema operativo o los programas intermedios), mientras que el cliente asumiría responsabilidad respecto de todos los componentes que le pertenecieran, como las aplicaciones que se ejecutaran utilizando esas infraestructuras o plataformas y los datos alojados en ellas.

Condiciones estándar del proveedor

132. En sus condiciones estándar, los proveedores pueden eximirse de toda responsabilidad contractual y adoptar la postura de que las cláusulas de responsabilidad son innegociables. Otra posibilidad es que el proveedor esté dispuesto a asumir responsabilidad, incluso ilimitada, por los incumplimientos que dependen de su voluntad (por ejemplo, una violación de las licencias de PI concedidas por el cliente al proveedor), pero no por los incumplimientos que puedan ocurrir por causas ajenas a su voluntad (por ejemplo, debido a hechos imprevisibles o a la filtración de información confidencial).

133. Por lo general, en las condiciones estándar de los proveedores, estos se eximen de responsabilidad por daños indirectos o emergentes (por ejemplo, la pérdida de oportunidades comerciales a raíz de la falta de disponibilidad de los servicios de computación en la nube). Cuando los proveedores asumen responsabilidad con carácter general o en determinados casos establecidos expresamente, en sus condiciones estándar se suele limitar la cuantía de los daños

por los que se responderá (por cada siniestro, serie de siniestros relacionados entre sí o período de tiempo). Además, los proveedores suelen fijar un límite máximo general a su responsabilidad contractual, que puede establecerse en función de los ingresos que esperan obtener de conformidad con el contrato, de su volumen de facturación o de la cobertura prevista en sus pólizas de seguro.

134. Normalmente, en las condiciones estándar de los proveedores se hace responsable al cliente del incumplimiento de la **PUA**.

Posibles variaciones de las condiciones estándar

135. Algunos hechos (por ejemplo, el quebrantamiento de las normas de protección de los **datos personales** y la vulneración de derechos de PI) podrían dar lugar a que cualquiera de las partes incurriera en un grado posiblemente alto de responsabilidad frente a terceros o a que se impusieran multas reglamentarias. Es habitual que se pacte un régimen de responsabilidad más severo (responsabilidad ilimitada o indemnizaciones más elevadas) para los casos en que el hecho sea imputable a la culpa o negligencia de la otra parte.

136. Tanto la ley como el contrato pueden limitar o excluir la responsabilidad de las partes por los actos de terceros que escapen a su control (por ejemplo, la responsabilidad del cliente por los actos de sus usuarios finales o la responsabilidad del proveedor por los actos del cliente o los usuarios finales de este).

Seguro de responsabilidad civil

137. En el contrato pueden preverse determinadas obligaciones en materia de seguros para una o ambas partes, especialmente en lo que respecta a los requisitos de calidad que deberá reunir la compañía de seguros elegida y la cuantía mínima de la cobertura que deberá obtenerse. También se puede establecer la obligación de cada parte de notificar a la otra los cambios que se realicen en la cobertura de su seguro o de proporcionar a la otra una copia de las pólizas de seguros que tenga en vigor.

K. MEDIDAS QUE PUEDEN ADOPTARSE EN CASO DE INCUMPLIMIENTO DEL CONTRATO

Tipos de medidas

138. Las partes pueden elegir libremente, dentro de los límites que establezca la ley aplicable, las medidas que adoptarán, entre ellas, por ejemplo,

medidas de reparación en especie que permitan a la parte agraviada obtener una prestación idéntica o equivalente a la que esperaba obtener en el marco del cumplimiento del contrato (por ejemplo, la sustitución del equipo físico defectuoso), compensaciones pecuniarias (por ejemplo, créditos para la utilización de servicios) y la resolución del contrato. En el contrato se podrían contemplar diferentes tipos de incumplimiento y especificar las medidas que podrían adoptarse en cada caso.

Suspensión o cancelación de los servicios

139. Una de las medidas que suele adoptar el proveedor cuando el cliente incumple el contrato o sus usuarios finales infringen la **PUA** es suspender o cancelar la prestación de los servicios de computación en la nube. En el contrato pueden preverse medidas de salvaguardia para restringir el alcance de los derechos de suspensión o cancelación de los servicios. Por ejemplo, el derecho del proveedor a suspender o cancelar la prestación de los servicios de computación en la nube al cliente puede limitarse a los casos en que este incurra en un incumplimiento esencial del contrato o en que surjan amenazas graves para la seguridad o la integridad del sistema del proveedor, así como a otros supuestos establecidos en la ley aplicable. El derecho del proveedor a suspender o cancelar los servicios también puede limitarse exclusivamente a los servicios que resulten afectados por el incumplimiento, cuando exista esa posibilidad.

Créditos para la utilización de servicios

140. Un mecanismo que suele utilizarse para compensar al cliente por el incumplimiento del proveedor es el sistema de créditos para la utilización de servicios. Esos créditos consisten en un descuento en el precio de los servicios contratados que se prestarán en el siguiente período de facturación. Se puede aplicar una escala variable (es decir, descontar un porcentaje que puede depender de la medida en que el servicio prestado por el proveedor en el marco del contrato no se ajuste a los parámetros de cantidad y calidad establecidos en el **SLA** o en otras partes del contrato). También se puede aplicar un límite máximo general a los créditos para la utilización de servicios. Los proveedores pueden limitar los casos en que se concederán esos créditos y disponer, por ejemplo, que solo los concederán cuando los fallos se deban a cuestiones que dependan de su voluntad o cuando el cliente reclame dichos créditos dentro de un plazo determinado. Algunos proveedores también pueden estar dispuestos a devolver sumas ya abonadas o a ofrecer un paquete de servicios mejorado durante el siguiente período de facturación (ofreciendo, por ejemplo, consultoría gratuita sobre tecnología de la información). Si existen varias medidas disponibles, es posible que en las condiciones estándar de los proveedores se

establezca que, en caso de incumplimiento del proveedor, este tendrá derecho a elegir la forma de subsanar su incumplimiento.

141. Cuando los créditos para la utilización de servicios son la única medida prevista para el caso de incumplimiento de las obligaciones contractuales del proveedor, el cliente puede ver limitado su derecho a recurrir a otras medidas, como la interposición de una demanda por daños y perjuicios o la resolución del contrato. Además, la concesión de créditos en forma de descuento en el precio de los servicios contratados o el ofrecimiento de un paquete de servicios mejorado en el período de facturación siguiente puede resultar inútil si se resuelve el contrato. Quizás no sea posible exigir el cumplimiento de una cantidad excesiva de créditos concedidos para la utilización de servicios si se considera que la estimación de los posibles daños futuros realizada al comienzo del contrato no fue razonable. Otras medidas, como la inclusión de una cláusula penal (cuando es admisible) o la fijación del monto de la indemnización en el contrato pueden constituir incentivos más adecuados para que este se cumpla.

Formalidades que han de seguirse en caso de incumplimiento del contrato

142. En el contrato pueden establecerse las formalidades que deben seguirse en caso de incumplimiento. Por ejemplo, en el contrato podría establecerse que la parte que considere que se ha infringido alguna cláusula del contrato deberá notificar a la otra esa circunstancia y darle la posibilidad de subsanar el incumplimiento aducido. También se pueden fijar plazos para solicitar las medidas pertinentes.

L. PLAZO Y EXTINCIÓN DEL CONTRATO

Fecha efectiva de entrada en vigor del contrato

143. La fecha efectiva de entrada en vigor del contrato puede no coincidir con la fecha en que este se firme, o con la fecha en que se acepte la oferta, o con la fecha en que se acepten la configuración y demás medidas necesarias para que el cliente migre sus contenidos a la nube. Puede considerarse que el contrato entra efectivamente en vigor en la fecha en que el proveedor pone a disposición del cliente los servicios de computación en la nube, aunque el cliente no llegue realmente a utilizarlos en ese momento. También puede considerarse que la fecha efectiva de entrada en vigor del contrato es aquella en que el cliente realiza el primer pago por los servicios de computación en la nube, aun cuando el proveedor no los haya puesto aún a su disposición. Por

esas razones, y para evitar dudas, las partes pueden indicar en el contrato la fecha efectiva de entrada en vigor de este.

Duración del contrato

144. La duración del contrato puede ser corta, mediana o larga. En el caso de las **soluciones de nube genéricas y estandarizadas para múltiples suscriptores** es habitual que se fije en el contrato un plazo inicial determinado (corto o mediano), prorrogable automáticamente a menos que alguna de las partes decida poner fin a la relación contractual. El proveedor puede convenir en notificar al cliente cuando se aproxime la fecha de vencimiento del contrato. Es posible que en la decisión de renovar o no el contrato influyan diversos factores, entre ellos el riesgo de **dependencia** o de perder la oportunidad de contratar otros servicios en condiciones más favorables.

Resolución anticipada

145. En los contratos se suelen establecer otras causas, además del vencimiento del plazo estipulado, que pueden dar lugar a su extinción, como la conveniencia de las partes, el incumplimiento u otros motivos. Es posible que en el contrato se prevean las condiciones que regirán su resolución anticipada, entre ellas la obligación de enviar una notificación con suficiente antelación, la **reversibilidad** y otras obligaciones relativas a la finalización de los servicios (véanse los párrs. 157 a 167 *infra*).

Resolución por razones de conveniencia

146. En las condiciones estándar de los proveedores, sobre todo las relacionadas con la prestación de **soluciones de nube genéricas y estandarizadas para múltiples suscriptores**, estos suelen reservarse el derecho a poner fin al contrato en cualquier momento, aunque el cliente no haya incurrido en incumplimiento. Las partes pueden convenir en limitar las circunstancias en que se podrá ejercer ese derecho y obligar al proveedor a notificar al cliente con suficiente antelación su voluntad de poner fin al contrato.

147. El derecho del cliente a resolver el contrato por razones de conveniencia (es decir, aunque el proveedor no haya incurrido en incumplimiento) es especialmente frecuente en los contratos públicos. En esos casos, el proveedor puede exigir el pago de una indemnización por resolución anticipada. No obstante, la posibilidad de exigir ese pago a un organismo público puede estar restringida por la ley. En los contratos de duración indefinida, si bien es posi-

ble que los proveedores estén más dispuestos a aceptar que el cliente ponga fin al contrato por razones de mera conveniencia sin tener que pagar una indemnización, ello podría dar lugar también a que se fijara un precio más alto en el contrato.

Resolución por incumplimiento

148. Por lo general, el incumplimiento esencial del contrato es motivo fundado para resolverlo. A fin de evitar ambigüedades, las partes pueden definir en el contrato los supuestos que constituirán un incumplimiento esencial de este. El incumplimiento esencial del contrato por el proveedor puede consistir en la pérdida o el uso indebido de los datos, el quebrantamiento de las normas de protección de los **datos personales**, la frecuencia de los **incidentes de seguridad** (cuando se produzcan, por ejemplo, más de un determinado número de veces en cada período de facturación), la filtración de información confidencial y la indisponibilidad de los servicios en determinados momentos o durante un determinado período de tiempo. La falta de pago por el cliente y la transgresión de la **PUA** por este o sus usuarios finales son algunos de los motivos más comunes por los que los proveedores ponen fin a los contratos. El derecho de una parte a resolver el contrato puede estar sometido a la condición de que se realice una notificación previa, se celebren consultas de buena fe y se ofrezca la posibilidad de corregir la situación. La parte puede estar obligada, en virtud del contrato, a reanudar el cumplimiento de este una vez transcurrido un determinado número de días a partir del momento en que se hayan adoptado las medidas correctivas correspondientes.

149. En el contrato pueden establecerse las obligaciones relativas a la finalización de los servicios asumidas por el proveedor que subsistirán aunque el cliente incurra en un incumplimiento esencial del contrato, entre ellas la **reversibilidad** de los datos y otros contenidos del cliente (véanse los párrs. 157 a 167 *infra*).

Resolución por modificaciones inaceptables del contrato

150. Algunas modificaciones introducidas en el contrato por una de las partes pueden no ser aceptables para la otra y constituir una causa justificada de resolución del contrato. Podrían estar incluidas en esa categoría las modificaciones de los **requisitos de ubicación de los datos** o las condiciones de subcontratación. El contrato puede conferir al cliente el derecho a resolverlo en su totalidad cuando las modificaciones introducidas en él a raíz de una reestructuración de la cartera de servicios del proveedor tengan como resultado la cancelación o sustitución de algunos de esos servicios (véanse los párrs. 105 a 124 *supra* y el párr. 155 *infra*).

Resolución por insolvencia

151. Es posible que se detecte un riesgo de insolvencia en la etapa de evaluación de los riesgos (véase la primera parte, párr. 15 *j)*) y durante el período de vigencia del contrato si, por ejemplo, en este se exige la presentación de informes periódicos sobre la situación financiera de las partes. Las cláusulas que permiten poner fin al contrato en caso de insolvencia de una de las partes son bastante frecuentes, aunque puede haber normas imperativas en el régimen de la insolvencia que las dejen sin efecto.

152. Un cliente insolvente quizás necesite seguir utilizando los servicios de computación en la nube mientras resuelve sus dificultades financieras. Las partes pueden limitar su derecho a invocar la insolvencia como único motivo para poner fin al contrato cuando no concurriera otro, por ejemplo, el incumplimiento de las obligaciones de pago contraídas por el cliente en virtud del contrato.

153. Puede haber mecanismos, ya sea estipulados por las partes en el contrato o establecidos en la ley, que permitan recuperar los datos del cliente en caso de insolvencia del proveedor (por ejemplo, la comunicación automática al cliente del código fuente o las claves bajo custodia para que este pueda acceder a sus datos y otros contenidos). Sin estos mecanismos, el cliente podría tener dificultades para recuperar sus datos y otros contenidos alojados en la infraestructura de nube del proveedor insolvente o tardar en recuperarlos. Cuando se produce un éxodo masivo y se retira una gran cantidad de contenidos como consecuencia de una crisis de confianza ocasionada por la situación financiera del proveedor, el proveedor insolvente o un **representante de la insolvencia** pueden limitar la cantidad de contenido (datos y código de las aplicaciones) que se podrá retirar en un período determinado, o decidir que las obligaciones relativas a la finalización de los servicios se irán cumpliendo en el orden en que se reciban las solicitudes correspondientes.

Resolución por cambio de control

154. El cambio de control puede ocurrir, por ejemplo, cuando cambia la propiedad de la empresa, o cuando cambia la capacidad de determinar, directa o indirectamente, las políticas operacionales y financieras del proveedor, lo que a su vez puede determinar que se modifique la cartera de servicios que este ofrece. El cambio de control puede producirse también cuando se realiza una cesión o una novación del contrato y se transmiten a un tercero los derechos y obligaciones (o solo los derechos) previstos en él. Como resultado de ello, es posible que cambie alguna de las partes contratantes originales o que se modifiquen determinados aspectos del contrato, de modo que, por ejemplo, los pagos tengan que realizarse a un tercero.

155. La ley aplicable puede disponer que se resuelva el contrato si, como consecuencia del cambio de control, no pudieran cumplirse los requisitos exigidos por normas legales imperativas (por ejemplo, los **requisitos de ubicación de los datos** o la prohibición de hacer negocios con determinadas entidades comprendidas en un régimen internacional de sanciones o por motivos de seguridad nacional). Los contratos públicos pueden verse especialmente afectados por restricciones legales aplicables a los cambios de control. Además, las partes pueden convenir en que se resuelva el contrato en caso de cambio de control, en especial si, como consecuencia de dicho cambio, un competidor del cliente adquiere la empresa del proveedor o lo sucede como parte en el contrato, o si el cambio de control tiene como resultado la interrupción o una modificación importante de los servicios comprendidos en la cartera. Es frecuente que se establezca la obligación de notificar con antelación todo cambio de control que se vaya a realizar próximamente, así como los efectos que se prevé que tenga el cambio sobre el contrato.

Cláusula sobre cuentas inactivas

156. La inactividad del cliente durante un determinado período de tiempo establecido en el contrato puede ser invocada por el proveedor como causa de resolución unilateral del contrato. Sin embargo, no es habitual que se incluya la cláusula sobre cuentas inactivas en los contratos de servicios remunerados de computación en la nube celebrados entre empresas.

M. OBLIGACIONES RELATIVAS A LA FINALIZACIÓN DE LOS SERVICIOS

157. Es posible que las obligaciones relativas a la finalización de los servicios no solo planteen dificultades de carácter contractual, sino también en relación con la normativa. Las partes pueden tratar de lograr un equilibrio entre, por una parte, el interés del cliente en disponer de acceso continuo a sus datos y otros contenidos (incluso durante el período de transición) y, por otra, el interés del proveedor en poner fin lo antes posible a toda obligación que pudiera vincularlo a su antiguo cliente.

158. Las obligaciones relativas a la finalización de los servicios pueden ser las mismas cualquiera sea la causa de extinción del contrato, o pueden variar según si el contrato se resuelve por incumplimiento o por otros motivos. En los párrafos siguientes se examinan una serie de cuestiones que las partes tal vez deseen prever en el contrato.

Plazo para la exportación

159. Las partes pueden estipular en el contrato un plazo para la exportación de los datos y otros contenidos del cliente, que quizás tenga que ser suficientemente amplio para que este pueda transferirlos sin dificultades a otro sistema.

Acceso del cliente al contenido que se ha de exportar

160. En el contrato deberían especificarse los datos y otros contenidos que habrán de exportarse, así como la forma en que el cliente podrá acceder a ellos, incluidas las claves de descifrado que pudieran estar en poder del proveedor o de terceros (véase la primera parte, párr. 28). A fin de facilitar la exportación de los datos del cliente con la mínima intervención del proveedor, las partes pueden pactar un sistema de custodia (es decir, la intervención de un tercero autorizado a comunicar automáticamente al cliente el código fuente, las claves de descifrado u otros elementos que le permitan recuperar sus datos y otros contenidos cuando se produzcan determinados hechos, como la extinción del contrato (véase también el párr. 153 *supra*)). En el contrato también pueden describirse distintas opciones para la exportación, indicando, en la medida de lo posible, sus respectivos formatos y procesos, aunque aclarando que pueden cambiar con el tiempo.

Asistencia prestada por el proveedor para la exportación

161. Si bien es posible que el proveedor no siempre esté dispuesto a ayudar activamente al cliente a exportar sus datos a otro sistema, la ley podría obligarlo a garantizar que esa exportación sea factible y fácil de realizar. Si las partes hubieran convenido en que el proveedor participase en la exportación de los datos del cliente a otro sistema, es posible que se especifiquen en el contrato los detalles de la asistencia que se prestará para la exportación, entre ellos, por ejemplo, el alcance de esa asistencia, el período en que tendrá lugar y el procedimiento que se seguirá para prestarla. El proveedor puede exigir un pago aparte por la prestación de asistencia para la exportación. En ese caso, las partes pueden establecer en el contrato la suma que deberá pagarse por esa asistencia, o convenir en remitirse al listado de precios del proveedor que esté vigente en un momento dado. Otra opción sería que las partes estipularan que esa asistencia quedara incluida en el precio del contrato o que no se cobrara ninguna suma adicional si el contrato se resolviera por incumplimiento del proveedor.

Eliminación de datos

162. Tal vez sea necesario estipular en el contrato las normas que regirán la **eliminación de datos** de la infraestructura de nube del proveedor una vez realizada su exportación o cuando haya vencido el plazo establecido en el contrato para llevar a cabo dicha exportación. El proveedor puede eliminar los datos automáticamente, por ejemplo, cuando se produzcan determinados hechos, venzan los plazos acordados por las partes o lo exija la ley. Como alternativa a lo anterior, podría estipularse que los datos se eliminasen solo cuando el cliente lo solicitara expresamente y siguiendo sus instrucciones específicas. Las partes pueden convenir en que se notifique al cliente cuando se aproxime la fecha de eliminación de los datos y se le entregue un certificado, informe o declaración sobre los datos eliminados, incluidos los que estuvieran alojados en sistemas de terceros.

Conservación de los datos una vez extinguido el contrato

163. El proveedor podría estar obligado a conservar los datos del cliente por disposición de la ley, en particular una ley dictada en materia de protección de datos, en la que también podría estar fijado el tiempo durante el cual deben conservarse los datos. La necesidad de conservar y almacenar certificados de firma digital, especialmente en el contexto transfronterizo, podría plantear algunos problemas concretos y dar lugar a que se impusieran determinadas obligaciones. Las partes pueden acordar que el proveedor conserve los datos del cliente una vez extinguido el contrato. Es posible que algunos proveedores ofrezcan, por un precio adicional, un servicio de conservación de los datos por un período determinado a partir de la extinción del contrato.

164. Las partes pueden establecer determinadas obligaciones respecto de los datos que no se devolverán o no podrán devolverse al cliente y cuya eliminación no sea posible. Por ejemplo, en el contrato puede estipularse que toda información personal deberá anonimizarse y que los datos se conservarán cifrados o en un formato utilizable e interoperable que permita recuperarlos si fuera necesario. Las partes pueden pactar también la responsabilidad que le incumbirá a cada una de ellas en lo que respecta a la conservación de los datos en el formato especificado una vez extinguido el contrato.

Cláusula de confidencialidad postcontractual

165. Las partes pueden pactar una cláusula de confidencialidad para la etapa posterior al contrato. En función de la naturaleza de los datos y otros conteni-

dos del cliente que se hayan alojado en la infraestructura de nube del proveedor, las obligaciones de confidencialidad pueden seguir existiendo durante un determinado número de años con posterioridad a la extinción del contrato (por ejemplo, de cinco a siete años) o prolongarse indefinidamente.

Auditorías posteriores a la extinción del contrato

166. Las auditorías posteriores a la extinción del contrato pueden ser acordadas por las partes o impuestas por la ley. Las partes pueden estipular las condiciones aplicables a esas auditorías, en particular el momento en que se llevarán a cabo y la forma en que se distribuirán sus costos.

Saldo remanente en cuenta

167. 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 o para que estas se compensen con las sumas adicionales que el cliente tuviera que abonar al proveedor, por ejemplo, por las actividades relativas a la finalización de los servicios o en concepto de indemnización de daños y perjuicios.

N. SOLUCIÓN DE CONTROVERSIAS

Mecanismos de solución de controversias

168. Las partes pueden acordar el método que utilizarán para resolver sus controversias contractuales. Los métodos de solución de controversias son, entre otros, la negociación, la mediación, la solución de controversias en línea (ODR), el arbitraje y la vía judicial. Según el tipo de controversia de que se trate, puede ser más conveniente recurrir a un tipo de procedimiento que a otro. Por ejemplo, es posible que las controversias sobre cuestiones financieras y técnicas se sometan a la decisión vinculante de un perito independiente (que puede ser una persona física o jurídica), mientras que para dirimir otro tipo de controversias puede ser más eficaz recurrir a las negociaciones directas entre las partes. En el caso de reclamaciones de menor cuantía, la mediación o la negociación asistidas por sistemas ODR pueden ofrecer a las partes métodos rápidos y económicos de alcanzar un acuerdo consensuado en línea. Para las reclamaciones de mayor cuantía, los sistemas ODR específicos del sector de la computación en la nube pueden constituir un foro especializado y competente y resultar de utilidad en los procesos judiciales. Es posible que en la legislación vigente en algunas jurisdicciones

se establezcan determinados mecanismos alternativos de solución de controversias que las partes tengan que agotar antes de poder someter su controversia a un órgano jurisdiccional.

Arbitraje

169. Las controversias que no se resuelvan de manera amistosa pueden someterse a arbitraje si las partes optaron por ese mecanismo. Sin embargo, no todas las controversias son susceptibles de someterse a arbitraje; la ley puede disponer que algunas de ellas solo puedan ser dirimidas por un órgano jurisdiccional. Por consiguiente, las partes deberían verificar si su controversia puede someterse a arbitraje antes de optar por esa vía. Cuando se incluye una cláusula de arbitraje en un contrato, normalmente se especifica en ella el reglamento de arbitraje que se aplicará al proceso arbitral. También puede incluirse en el contrato una cláusula estándar de solución de controversias que disponga la aplicación de normas reconocidas internacionalmente para llevar a cabo el proceso en cuestión (por ejemplo, el Reglamento de Arbitraje de la CNUDMI). A falta de una disposición contractual en tal sentido, el proceso arbitral se regirá normalmente por el derecho procesal del Estado en que tenga lugar o, si las partes hubieran elegido una institución arbitral, por el reglamento de esta.

Solución de controversias en línea

170. Las partes pueden optar por un mecanismo ODR para resolver todas las clases de controversias que se deriven de su contrato, o solo algunas de ellas, a reserva de las limitaciones establecidas en la ley. En el contrato pueden especificarse el alcance de las cuestiones que podrán someterse a un sistema ODR, la plataforma ODR que se utilizará y el reglamento por el que se regirá el proceso. En algunos casos, la opción de resolver las controversias en línea podría estar incluida en el paquete de servicios de nube ofrecido por el proveedor, con la posibilidad de renunciar a ella voluntariamente.

171. El proceso ODR suele estar compuesto de las siguientes etapas: *a)* negociaciones celebradas entre las partes por conducto de la plataforma ODR; *b)* arreglo facilitado, en que se nombra a un tercero neutral que se comunica con las partes para tratar de que lleguen a un arreglo; y *c)* una etapa final, en que el administrador de servicios ODR o un tercero neutral informan a las partes de la naturaleza y forma de la etapa final. El resultado del proceso ODR puede no ser vinculante para las partes, a menos que el contrato o la ley aplicable dispongan lo contrario.

Vía judicial

172. Si se entablara un proceso judicial podría suceder que, debido a la naturaleza de los **servicios de computación en la nube**, varios Estados se declarasen competentes para entender en el litigio. En la medida de lo posible, es conveniente que las partes se pongan de acuerdo sobre una cláusula de competencia que las obligue a someter sus controversias a un determinado órgano jurisdiccional (véanse los párrs. 175 a 181 *infra*).

Conservación de datos

173. Durante la fase de solución de la controversia puede resultar vital que el cliente tenga acceso continuado a sus datos, incluidos los **metadatos** y otros **datos obtenidos de los servicios de nube**, no solo para garantizar la continuidad de sus operaciones, sino también a los efectos de su participación en el proceso en cuestión (por ejemplo, para fundamentar una demanda o una reconvención). En el contrato puede estipularse expresamente que, en caso de que surjan controversias entre las partes, el proveedor conservará los datos del cliente y este último tendrá acceso a sus datos durante un período de tiempo razonable, con independencia de la naturaleza de la controversia. Las partes también pueden pactar un sistema de custodia (véase el párr. 160 *supra*).

Plazo de prescripción para la presentación de reclamaciones

174. Las partes pueden fijar en el contrato el plazo en que podrán presentarse reclamaciones. No obstante, si resultaran aplicables los plazos de prescripción establecidos en la ley, las estipulaciones contractuales que no se ajustaran a esos plazos quedarían sin efecto.

O. CLÁUSULAS DE ELECCIÓN DE LA LEY Y EL FORO

175. Con arreglo al principio de la libertad contractual (véase el párr. 34 *supra*), normalmente las partes pueden elegir la ley que será aplicable a su contrato y la jurisdicción o el foro en que se examinarán sus controversias. No obstante, y en función del objeto de la controversia de que se trate, es posible que existan normas legales imperativas (por ejemplo, en materia de protección de datos) que prevalezcan sobre las cláusulas de elección de la ley y el foro que hayan pactado las partes contratantes. Además, independientemente de la ley y el foro que las partes elijan, es posible que sean aplicables al contrato más de un conjunto de normas legales imperativas (por ejemplo, las normas en

materia de protección de datos y el régimen legal de la insolvencia), incluso de diferentes jurisdicciones.

Cuestiones que deben tenerse en cuenta al elegir la ley aplicable y el foro

176. Las cláusulas de elección de la ley y el foro están relacionadas entre sí. La aplicación de la ley elegida y convenida dependerá, en última instancia, del foro en que se invoque la cláusula de elección de la ley ante un órgano jurisdiccional u otro órgano decisor (por ejemplo, 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 aplicable que hayan hecho las partes. Dada la importancia que tiene la ley del foro para la aplicabilidad de la cláusula de elección de la ley, en los contratos que contienen dicha cláusula también se suele incluir una cláusula de elección del foro.

177. Al elegir el foro, las partes suelen tener en cuenta los efectos de la ley aplicable que hayan elegido o de la ley que resulte aplicable por otros motivos y la medida en que se reconocerá y aplicará una resolución judicial de ese foro en los países en los que probablemente se solicite su ejecución. Quizás sea importante mantener la flexibilidad en cuanto a los métodos de ejecución por los que se puede optar, especialmente en los entornos de computación en la nube en que puede resultar difícil determinar muchos de los factores que las partes suelen tener en cuenta al redactar las cláusulas de elección de la ley y el foro, como el lugar en que se encuentran los bienes utilizados para la prestación de los servicios, el proveedor y el cliente.

Ley y foro obligatorios

178. Es posible que sea obligatorio someterse a la ley y el foro de una determinada jurisdicción por diversos motivos, entre ellos los siguientes:

a) La accesibilidad de los servicios de computación en la nube en el territorio de un Estado determinado puede ser suficiente para que resulten aplicables las leyes sobre protección de datos de ese Estado;

b) La nacionalidad o el domicilio del **sujeto de los datos** que se ha visto afectado o de las partes contratantes, en especial del **responsable de los datos**, pueden dar lugar a la aplicación de la ley de ese **sujeto de los datos** o de esa parte; y

c) La ley del lugar en que se originó la actividad (la ubicación del equipo) o al que se dirige la actividad con fines de lucro puede hacer necesario aplicar

la ley de ese lugar. Entre los factores que podrían tenerse en cuenta para determinar si será aplicable esa ley figuran la utilización de un dominio de nivel superior de un determinado país vinculado a un lugar determinado, el uso del idioma local en un sitio web, la fijación de los precios en la moneda local y la mención de personas de contacto locales.

Ley y foro del proveedor o del cliente

179. En los contratos de **soluciones de nube genéricas y estandarizadas para múltiples suscriptores** se suele establecer que se regirán por la ley del lugar de ubicación del establecimiento o domicilio comercial principal del proveedor. En esos contratos se otorga normalmente a los órganos jurisdiccionales del país del proveedor competencia exclusiva sobre todas las controversias derivadas del contrato. El cliente quizás prefiera la ley y el foro de su propio país. Por lo general, las instituciones públicas tienen importantes restricciones para aceptar la ley de otros países y la competencia de tribunales extranjeros. Es posible que los proveedores que operan en múltiples jurisdicciones muestren flexibilidad en lo que respecta a aceptar la ley y el foro del país en que se encuentra el cliente.

Multiplicidad de opciones

180. Las partes también pueden elegir leyes y foros diferentes para distintos aspectos del contrato. Asimismo, pueden optar por la jurisdicción del demandado, para que el demandante no tenga la ventaja de poder litigar ante el foro de su propio país, fomentando así las vías oficiosas de solución de controversias.

Ausencia de cláusulas de elección de la ley y el foro

181. Las partes pueden preferir no incluir cláusulas de elección de la ley y el foro en su contrato, dejando abierta la cuestión para que se discuta más adelante, si fuera necesario. En algunos casos, esta podría considerarse la única solución viable. El sistema ODR también puede ser útil para resolver las cuestiones de competencia y ley aplicable (véanse los párrs. 170 y 171).

P. NOTIFICACIONES

182. En las cláusulas relativas a las notificaciones se suelen establecer 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 (en el momento de la entrega, del envío o del acuse de recibo). A falta de disposiciones legales imperativas al respecto, las partes pueden acordar las formalidades a que deben ajustarse las notificaciones, que pueden ser uniformes o variar en función de su importancia, su urgencia y otras consideraciones. Es posible que para determinadas notificaciones, como las relativas a la suspensión o a la resolución unilateral del contrato, se exijan formalidades más estrictas que para las notificaciones ordinarias. Las partes pueden pactar los plazos de notificación, teniendo presente la necesidad de garantizar la **reversibilidad** y la continuidad de las operaciones. En el contrato puede hacerse referencia a las notificaciones y plazos impuestos por la ley.

183. Las partes pueden decidir que las notificaciones se realicen por **escrito** y se envíen a la dirección electrónica o se entreguen en la dirección física de las personas de contacto indicadas en el contrato. Es posible que en el contrato se establezcan los efectos jurídicos de no notificar o no responder a una notificación a la que deba contestarse.

Q. OTRAS CLÁUSULAS

184. A menudo las partes agrupan bajo el título "otras cláusulas" diversas estipulaciones 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 utilizarse en toda clase de contratos mercantiles, como la cláusula de divisibilidad, que permite excluir del contrato las disposiciones nulas, o la cláusula en que se establece que la versión del contrato redactada en un determinado idioma es la que prevalecerá sobre las versiones en los demás idiomas en caso de que hubiera discrepancias respecto de su interpretación. El hecho de que una cláusula figure entre las denominadas "otras cláusulas" del contrato no disminuye su importancia desde el punto de vista jurídico. Las partes pueden adaptar algunas de ellas teniendo en cuenta las particularidades de los **servicios de computación en la nube.**

R. MODIFICACIÓN DEL CONTRATO

185. Cualquiera de las partes puede proponer que se modifique el contrato. El procedimiento que debe seguirse para introducir modificaciones y para que estas surtan efecto suele estar previsto en el contrato. Quizás sea necesario prever también en el contrato las consecuencias de que alguna de las partes rechace las modificaciones.

186. Habida cuenta de la naturaleza de los **servicios de computación en la nube**, podría ser difícil distinguir entre los cambios que supondrían una modi-

ficación del contrato y los que no entrañarían tal modificación. Por ejemplo, la utilización por el cliente de cualquiera de las opciones previstas en el contrato desde el principio no sería necesariamente una modificación del contrato inicial, como tampoco lo serían los cambios que se hicieran en los servicios como resultado de operaciones rutinarias de mantenimiento y otras actividades del proveedor previstas en el contrato (véanse los párrs. 105 y 106 *supra*). En cambio, el hecho de añadir funcionalidades no previstas en las condiciones acordadas inicialmente, que por ende justifiquen un ajuste en el precio, puede constituir una modificación del contrato. Las actualizaciones que den lugar a cambios sustanciales en las condiciones y políticas acordadas previamente también pueden constituir una modificación del contrato.

187. El alcance de las modificaciones que se permite introducir en los contratos públicos puede estar limitado 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 celebrado en virtud de un procedimiento de licitación pública.

188. En caso de que se modificaran con frecuencia las condiciones pactadas originalmente, podría ser conveniente que cada una de las partes guardara separadamente el texto íntegro de las condiciones iniciales y de sus modificaciones.

Glosario

Acuerdo de prestación de servicios (**SLA**): parte del contrato de computación en la nube celebrado entre el proveedor y el cliente en la que se describen los servicios de computación en la nube comprendidos en el contrato y los parámetros a que se espera o se exige que se ajusten esos servicios de conformidad con el contrato (véase la definición de **parámetros cuantitativos y cualitativos**).

Aprovechamiento de los 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 los servicios de manera ininterrumpida y reducir al mínimo la distancia media entre los servidores y los usuarios finales a fin de disminuir la **latencia** y aumentar al máximo la velocidad de transmisión de los datos entre un dispositivo y otro (velocidad de transferencia de datos o caudal de datos).

Auditoría: proceso consistente en examinar el cumplimiento de los requisitos legales y contractuales o de normas técnicas. 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 o el uso del sistema sin autorización y garantizar la integridad de los datos. La auditoría puede ser interna o externa, o llevarse a cabo por un tercero independiente nombrado por el proveedor, el cliente o ambos. En el **acuerdo de prestación de servicios** (**SLA**) pueden establecerse parámetros cuantitativos y cualitativos específicos relacionados con la auditoría, por ejemplo, que un auditor independiente certifique, al menos una vez al año, que los servicios prestados en virtud del contrato cumplen una norma de seguridad indicada en el propio contrato.

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 colaboran en las actividades del proveedor, del cliente o de ambos, prestando servicios auxiliares o de apoyo a esas actividades. Los auditores de servicios de nube realizan la **auditoría** de la prestación y utilización de los **servicios de computación en la nube**. Los intermedia-

rios de servicios de nube o los integradores de sistemas prestan asistencia a las partes en relación con una amplia gama de cuestiones, por ejemplo, para encontrar la solución de nube más adecuada, negociar condiciones aceptables y migrar los datos y contenidos del cliente a la nube.

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

Datos personales: datos confidenciales y no confidenciales que pueden utilizarse para identificar a la persona física a la que se refieren esos datos. La definición de **datos personales** en algunas jurisdicciones puede abarcar cualquier dato o información directa o indirectamente vinculada o relacionada con una persona que haya sido o pueda ser identificada (véase la definición de **sujeto de los datos**).

Dependencia (*lock-in*): situación en que el cliente depende de un único proveedor porque el costo de cambiar a otro sería demasiado alto. En este contexto, el costo debe entenderse en el sentido más amplio posible, de modo que abarque no solo el costo económico, sino también el costo en términos de esfuerzo, tiempo y relaciones.

Derechos de los sujetos de los datos: derechos vinculados a los **datos personales de los sujetos de los datos**. La ley puede otorgar a los **sujetos de los datos** el derecho a ser informados de todos los hechos importantes que guarden relación con sus **datos personales**, como la ubicación de esos datos, su utilización por terceros, la filtración de datos u otras violaciones de los datos. Los **sujetos de los datos** también pueden tener derecho a acceder en cualquier momento a sus **datos personales,** a que esos datos se eliminen (en virtud del derecho al olvido), a restringir su **procesamiento** y a que se les garantice la **portabilidad** de dichos datos.

Eliminación de datos: secuencia de operaciones diseñadas para borrar datos de forma irreversible, incluidas sus copias de seguridad, metadatos y otros contenidos de la infraestructura (física y virtual) de computación en la nube. En algunos casos puede ser necesario, para eliminar los datos, destruir la infraestructura física (por ejemplo, los servidores) en que se almacenaron. En el **acuerdo de prestación de servicios** (**SLA**) puede establecerse un paráme-

tro cuantitativo o cualitativo específico aplicable a la eliminación de datos, por ejemplo, que el proveedor garantice que los datos del cliente se eliminen de manera efectiva, irrevocable y permanente cuando este lo solicite, en un plazo establecido en el contrato y de conformidad con la norma o el método indicados en él.

Escrito o **por escrito**: información que sea accesible de modo que pueda utilizarse para su ulterior consulta. Abarca tanto la información que figure en papel como la información contenida en una comunicación electrónica. "Accesible" significa que la información en formato electrónico debe poder leerse e interpretarse, y que los programas informáticos necesarios para que esa información pueda leerse deben conservarse. La posibilidad de "utilizar" la información se refiere tanto a su utilización por el ser humano como a su procesamiento informático.

Incidente de seguridad: hecho que indica que se ha quebrantado la seguridad del sistema o de los datos o que han fallado las medidas adoptadas para protegerlos. Un incidente de seguridad altera el funcionamiento normal del sistema. Son ejemplos de incidentes de seguridad los intentos de acceso no autorizados al sistema o a los datos, la interrupción imprevista de un servicio o la denegación de un servicio, el procesamiento o el almacenamiento no autorizados de datos y los cambios no autorizados en la infraestructura del sistema.

Infraestructura como servicio (**IaaS**): tipos de **servicios de computación en la nube** que permiten al cliente obtener y utilizar recursos de procesamiento, de almacenamiento o de redes. El cliente no administra ni controla los recursos virtuales ni los recursos físicos subyacentes, pero tiene el control de los sistemas operativos, el almacenamiento y las aplicaciones instaladas que utilizan esos recursos. Además, la capacidad del cliente de controlar determinados componentes de la red (por ejemplo, los cortafuegos locales) puede estar limitada.

Interoperabilidad: capacidad de dos o más sistemas o aplicaciones para intercambiar información entre sí y utilizar esa información.

Latencia: demora entre la solicitud del usuario y la respuesta del proveedor. Afecta a la utilidad real de los **servicios de computación en la nube**. En el **acuerdo de prestación de servicios** (**SLA**), la latencia suele expresarse en milisegundos.

Licencias de propiedad intelectual (**PI**): acuerdos celebrados entre un titular de derechos de PI (el licenciante) y una persona autorizada a utilizar esos derechos de PI (el licenciatario). En esos acuerdos se suelen imponer restricciones y obligaciones con respecto a la medida y la forma en que el licenciatario o

los terceros pueden utilizar la propiedad intelectual objeto de la licencia. Por ejemplo, se pueden conceder licencias para que se haga un uso específico de determinados programas informáticos y contenido visual (diseños, planos e imágenes), con la prohibición de realizar copias, modificaciones o mejoras de dichos programas y contenido y limitando su utilización a un determinado soporte. Las licencias pueden concederse exclusivamente para un mercado en particular (por ejemplo, nacional o (sub)regional) o un cierto número de usuarios o dispositivos, o por un plazo determinado. Es posible que no se permita conceder sublicencias. El licenciante puede exigir que cada vez que se utilicen los derechos de PI se mencione al titular de esos derechos.

Metadatos: información básica sobre los datos (como su autor, fecha y hora de creación y 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. Pueden ser generados por el cliente o el proveedor.

Modelos de despliegue: diversas formas de organizar los servicios de computación en la nube sobre la base del control y el uso compartido de los recursos físicos o virtuales. Cabe mencionar los 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 el control de los recursos es ejercido 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 el control de los recursos es ejercido por al menos uno de los miembros de ese grupo;

c) modelo de **nube privada**, en que un único cliente utiliza los **servicios de computación en la nube** y ejerce el control de los recursos;

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

Normativa propia de cada sector: normas aplicables a los sectores financiero, sanitario, público u otros sectores o profesiones concretos (por ejemplo, las normas relativas al secreto profesional que deben guardar los abogados y los médicos) y al manejo de la información de carácter reservado (entendida en sentido amplio como la información a la que, por disposición de una ley o un reglamento, solo pueden acceder determinadas categorías de personas).

Objetivos de punto de recuperación (**RPO**): 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 el

período establecido como RPO en el contrato abarca 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 en que existían dos horas antes de producirse la interrupción.

Objetivos de tiempo de recuperación (**RTO**): plazo máximo en que deben recuperarse todos los datos y servicios de computación en la nube a partir de que se produzca una interrupción imprevista.

Parámetros cuantitativos y cualitativos: parámetros cuantitativos (con objetivos, indicadores o rangos de valores numéricos de funcionamiento) o 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 (por ejemplo, que el proveedor haya aplicado una política de administración de claves en cumplimiento de las normas internacionales indicadas en el contrato). Para que tengan sentido, los parámetros deberían permitir al cliente evaluar, de manera sencilla y verificable, los aspectos del funcionamiento de los servicios que sean importantes para él. Pueden ser diferentes en función de los riesgos y 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 necesitará el mismo **período de disponibilidad** ni las mismas condiciones previstas en el **acuerdo de prestación de servicios** (**SLA**) que las operaciones esenciales o las operaciones en tiempo real.

Período de disponibilidad de los servicios: tiempo durante el cual es posible acceder a los servicios de computación en la nube y utilizarlos. Puede expresarse como una cantidad o un porcentaje, una fórmula detallada, o fechas concretas o días y horas específicos en que la disponibilidad del servicio correspondiente a una determinada aplicación resulta crítica.

Período de interrupción o **corte de los servicios**: 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**. El tiempo dedicado a las tareas de mantenimiento y actualización se suele incluir en el período de interrupción de los servicios. El **período de interrupción** o **corte de los servicios** puede definirse en el **acuerdo de prestación de servicios** (**SLA**) como el número de cortes permitidos de determinada duración en un lapso dado (por ejemplo, no más de un corte diario de una hora de duración y que no se produzca entre las 8.00 y las 17.00 horas).

Permanencia del almacenamiento de los datos: probabilidad de que los datos almacenados en la nube no se pierdan durante el período de vigencia

del contrato. Puede indicarse en el contrato como un objetivo mensurable que el cliente utilizará para evaluar las medidas adoptadas por el proveedor para garantizar que los datos permanezcan almacenados (por ejemplo, datos intactos/datos intactos + datos perdidos en un período determinado (por ejemplo, un mes natural)). Convendría definir en esa fórmula el tipo de datos (por ejemplo, archivos, bases de datos, códigos, aplicaciones) y la unidad de medida (el número de archivos, la longitud de bits).

Plataforma como servicio (**PaaS**): tipos de **servicios de computación en la nube** que permiten al cliente desplegar, administrar y ejecutar en la nube aplicaciones creadas o adquiridas por él utilizando al menos uno de los lenguajes de programación y entornos de ejecución ofrecidos por el proveedor.

Política de uso aceptable (**PUA**): parte del contrato de computación en la nube celebrado entre el proveedor y el cliente en la que se definen los límites del uso que podrán hacer el cliente y sus usuarios finales de los servicios de computación en la nube previstos en el contrato.

Portabilidad: capacidad de transferir datos, aplicaciones y otros contenidos de un sistema a otro fácilmente (es decir, a bajo costo, con el menor trastorno posible y sin necesidad de volver a introducir datos, reorganizar procesos o reprogramar aplicaciones). Esto podría lograrse si fuera posible recuperar los datos en un formato que fuese aceptado por otro sistema o mediante una transformación sencilla y directa utilizando herramientas que estén disponibles normalmente. En el **acuerdo de prestación de servicios** (**SLA**) pueden establecerse parámetros cuantitativos y cualitativos específicos relacionados con la portabilidad, por ejemplo, que el cliente pueda recuperar sus datos mediante un único enlace de descarga o interfaces de programación de aplicaciones (API) documentadas; o que el formato de los datos esté suficientemente estructurado y documentado para permitir que el cliente los vuelva a utilizar o los reestructure en un formato diferente, si así lo desea.

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

Programas informáticos como servicio (**SaaS**): tipos de **servicios de computación en la nube** que permiten al cliente utilizar las aplicaciones del proveedor en la nube.

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

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 entrañar la prohibición de alojar o trasladar determinados datos (como los **metadatos** y las copias de seguridad) dentro o fuera de una zona o jurisdicción determinada, o la obligación de obtener previamente la autorización de un órgano estatal competente para poder hacerlo. Suelen estar previstos en las leyes y reglamentos sobre protección de datos, que pueden establecer en particular la prohibición de alojar **datos personales** en jurisdicciones que no respeten determinadas normas de protección de **datos personales,** o de trasladar **datos personales** a esas jurisdicciones.

Responsable de los datos: persona que determina los objetivos y medios que han de emplearse para procesar **datos personales**.

Reversibilidad: proceso mediante el cual el cliente puede recuperar de la nube sus datos, aplicaciones y otros contenidos conexos y que permite al proveedor eliminar los datos y otros contenidos conexos del cliente una vez vencido el plazo acordado.

Servicios de computación en la nube: servicios en línea con las siguientes características:

a) **acceso amplio a la red**: significa que es posible acceder a los servicios 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) **sujetos a medición**: significa que se puede llevar un registro de los recursos utilizados y cobrarlos en función de su uso (conforme a un régimen de **pago por uso**);

c) **arrendamiento múltiple**: 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**: significa que el cliente utiliza los servicios cuando los necesita, de manera automática o con una interacción mínima con el proveedor;

e) **elasticidad** y **escalabilidad**: capacidad de ampliar o reducir rápidamente el consumo de los servicios en función de las necesidades del cliente, teniendo en cuenta las grandes tendencias en la utilización de los recursos (por ejemplo, los efectos estacionales);

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

g) **amplia gama de servicios**: abarca desde el suministro y la utilización de la conectividad y los servicios informáticos básicos (como el almacenamiento, el correo electrónico y las aplicaciones de oficina), hasta el suministro y la utilización 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 que el cliente construya sus propias plataformas de tecnología de la información, o despliegue, administre y ejecute las aplicaciones o los programas informáticos creados o adquiridos por él. La infraestructura como servicio (**IaaS**), la plataforma como servicio (**PaaS**) o los programas informáticos como servicio (**Saas**) son tipos de servicios de computación en la nube.

Servicios estratificados de computación en la nube: servicios en que el proveedor no es propietario de la totalidad o algunos de los recursos de computación que utiliza para prestar los servicios de computación en la nube a sus clientes, sino que él es, a su vez, cliente de la totalidad o algunos de los **servicios de computación en la nube**. Por ejemplo, el proveedor de servicios de tipo **PaaS** o **SaaS** puede utilizar infraestructura de almacenamiento y servidores (centros de datos, servidores de datos) de propiedad de otra entidad o suministrados por otra entidad. Como resultado de ello, en la prestación de los servicios de computación en la nube al cliente podrían participar uno o más subproveedores. Es posible que el cliente no sepa qué proveedores o subproveedores 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**.

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 cláusulas que liberan o eximen ampliamente de responsabilidad al 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.

Sujeto de los datos: persona física cuya identidad puede determinarse, directa o indirectamente, a través de los datos, por ejemplo, por referencia a datos identificadores como el nombre, un número de identificación, la ubicación y otros factores relacionados con la identidad física, genética, mental, económica, cultural o social de la persona. En varias jurisdicciones, las normas sobre protección o privacidad de los datos confieren a los sujetos de los datos determinados derechos sobre los datos que permiten identificarlos. Esas nor-

mas pueden dar lugar a que se incluyan parámetros cuantitativos y cualitativos específicos sobre la protección de datos en el **acuerdo de prestación de servicios** (**SLA**), por ejemplo, que un auditor independiente certifique, al menos una vez al año, que los servicios prestados en virtud del contrato cumplen la norma sobre protección o privacidad de los datos indicada en el propio contrato. (Véanse también las definiciones de **derechos de los sujetos de los datos** y **datos personales**).

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

V.19-09106