Naciones Unidas A/CN.9/974

Asamblea General

Distr. general
27 de julio de 2018
Español
Original: inglés

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
52º período de sesiones
Viena, 8 a 26 de julio de 2019

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

Nota de la Secretaría

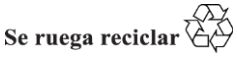
1. En su 51er período de sesiones, celebrado en 2018, la Comisión estudió la recomendación del Grupo de Trabajo IV (Comercio Electrónico) de que la Comisión examinara el proyecto de notas sobre las principales cuestiones relacionadas con los contratos de computación en la nube en su 52º período de sesiones, en 2019, y autorizara su publicación o emisión como instrumento de consulta en línea, en ambos casos como producto de la labor de la Secretaría (A/CN.9/936, párr. 44). Tras un debate, la Comisión decidió examinar el proyecto de notas sobre las principales cuestiones relacionadas con los contratos de computación en la nube en su 52º período de sesiones en 2019[1].

2. Asimismo, en su 51er período de sesiones, la Comisión pidió a la Secretaría que preparara, dentro de los recursos disponibles, una herramienta en línea de carácter experimental que incluyera el proyecto de notas sobre las principales cuestiones relacionadas con los contratos de computación en la nube, a fin de examinarla en su 52º período de sesiones en 2019. La Comisión también pidió a la Secretaría que preparara una nota con consideraciones relativas a la preparación de la herramienta en línea de carácter experimental, incluidas las consecuencias presupuestarias y de otra índole, e indicara en qué medida esa herramienta se apartaría de la política de publicaciones actual de la CNUDMI[2].

3. En el anexo de la presente nota figura el texto del proyecto de notas sobre las principales cuestiones relacionadas con los contratos de computación en la nube, preparado por la secretaría de la CNUDMI. Los términos destacados en negrita se describen en el glosario que figura al final del proyecto de notas. Por separado, en el documento A/CN.9/975, se presentará una nota de la Secretaría sobre la herramienta en línea de carácter experimental que incluirá el proyecto de notas sobre las principales cuestiones relacionadas con los contratos de computación en la nube.

[1] *Documentos Oficiales de la Asamblea General, septuagésimo tercer período de sesiones, Suplemento núm. 17* (A/73/17), párr. 150.
[2] *Ibid.*, párr. 155.

V.18-05200 (S) 041218 041218



Anexo

Notas sobre las principales cuestiones relacionadas con los contratos de computación en la nube (preparada por la secretaría de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, 2019)

Índice

Introducción

1. En estas notas se abordan las principales cuestiones que podrían plantear los contratos de computación en la nube celebrados por 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 el usuario 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. Asimismo, quedan excluidos de su ámbito de aplicación los contratos celebrados con **colaboradores de los servicios de computación en la nube** y otros terceros que puedan participar en la prestación de esos servicios al cliente (por ejemplo, los contratos celebrados con subcontratistas o proveedores de servicios de Internet).

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

3. Las cuestiones abordadas en estas notas pueden plantearse en los contratos de computación en la nube con independencia del tipo de **servicios de computación en la nube** de que se trate (por ejemplo, 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). Las notas se centran en los contratos de servicios de computación en la nube de tipo **SaaS** público con remuneración.

4. La capacidad para negociar las cláusulas de los contratos de computación en la nube dependerá de muchos factores, en especial de si el contrato versa sobre **soluciones de nube genéricas y estandarizadas para múltiples suscriptores** o sobre una solución personal, hecha a medida; de si existen o no ofertas competidoras, así como de las posiciones de negociación de las partes que quizás celebren el contrato. La capacidad para negociar las condiciones de un contrato (en especial las cláusulas sobre suspensión, rescisión o modificación unilaterales del contrato por parte del proveedor y las cláusulas de responsabilidad) puede ser un factor importante a la hora de elegir un proveedor en los casos en que es posible elegir. Aunque las notas han sido elaboradas 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 con el fin de determinar si dichas condiciones se ajustan a sus necesidades.

5. Estas 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 ellas se señalan algunas cuestiones que deberían tener en cuenta quienes consideren la posibilidad de suscribir un contrato, tanto antes como durante su redacción, sin pretender transmitir la idea de que todas esas cuestiones deban analizarse siempre. Las diversas soluciones que se examinan en estas notas no se aplicarán a las relaciones entre las partes a menos que estas las acepten expresamente, o a menos que las soluciones resulten de lo dispuesto en la ley aplicable. Ni los títulos ni los 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. 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 abordan los principales aspectos precontractuales que las futuras partes podrían 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 podrían 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 marco jurídico aplicable al cliente, al proveedor o a ambos puede imponer ciertas condiciones para la celebración de un contrato de computación en la nube. Esas condiciones pueden tener su origen también en obligaciones contractuales, como las que surgen de las **licencias de propiedad intelectual (PI)**. Las partes deben prestar especial atención a las leyes y reglamentos sobre **datos personales**, 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, como la nulidad o la inexigibilidad de la totalidad o una parte del contrato, multas administrativas y responsabilidad penal.

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

Ubicación de los datos

10. Los **requisitos de ubicación de los datos** pueden derivarse especialmente de la legislación aplicable en materia de **datos** personales, datos contables y datos del sector público, así como de las leyes y reglamentos de fiscalización de las exportaciones que pueden limitar la transmisión de determinados datos o programas informáticos hacia o desde determinados países o regiones. El cumplimiento de los requisitos de ubicación de los datos establecidos en la ley aplicable será de suma importancia para las partes. El contrato no podrá excluir la aplicación de esos requisitos.

11. Los **requisitos de ubicación de los datos** también pueden surgir de compromisos contractuales con terceros, por ejemplo, las **licencias de PI** que exigen que el contenido bajo licencia se almacene en los servidores seguros del propio usuario. Establecer requisitos de **ubicación de los datos** puede considerarse conveniente por meras razones prácticas, entre ellas, para reducir la **latencia**, algo que puede ser especialmente importante en las operaciones en tiempo real, como las operaciones bursátiles. (En cuanto a las medidas contractuales de salvaguardia 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 disposiciones reglamentarias. Es posible que la ley prohíba celebrar contratos de computación en la nube con personas o entidades extranjeras, de determinadas jurisdicciones o que no hayan sido acreditadas ante las autoridades competentes del Estado o no hayan recibido certificación de estas. Quizás la ley exija que la persona o entidad extranjera constituya una empresa mixta con una entidad nacional u obtenga licencias y permisos locales, como permisos de exportación, para poder prestar **servicios de computación en la nube** en una jurisdicción determinada. Los requisitos de **ubicación de los datos** (véanse los párrs. 10 y 11 *supra*), así como las obligaciones impuestas por la ley a cualquiera de las partes de revelar información o facilitar el acceso a los datos y otros contenidos a las autoridades de Estados extranjeros, también pueden influir en la elección de una parte contratante.

B. Evaluación precontractual de los riesgos

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

14. No todos los riesgos derivados de los contratos de computación en la nube son específicos de este campo. Algunos de ellos podrían tener que abordarse fuera del marco de un contrato de computación en la nube (por ejemplo, los riesgos derivados de las interrupciones en la conexión a Internet), y no todos pueden mitigarse a un costo aceptable (por ejemplo, el riesgo de deterioro de la reputación). Además, es posible que la evaluación de riesgos no se lleve a cabo de una sola vez antes de celebrar un contrato. Es posible que los riesgos se evalúen continuamente durante la vigencia del contrato y que de ello resulte la modificación o rescisión de este.

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 a la hora de examinar la utilización de determinados **servicios de computación en la nube** y seleccionar a una parte contratante:

a) las **licencias de PI** necesarias para utilizar determinados servicios 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 tratamiento, tránsito o transmisión mediante el uso de infraestructura de computación en la nube;

c) las medidas adoptadas para garantizar el acceso continuado a los **metadatos**, registros de auditoría y otros registros que demuestren la existencia de medidas de seguridad;

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 vigentes en lo que respecta a la asistencia prestada en los procesos de migración a la nube y finalización del servicio, así como en materia de **interoperabilidad** y **portabilidad**;

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

g) las estadísticas relativas a los **incidentes de seguridad** e información sobre la calidad del servicio 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**; y

n) el alcance del aislamiento de los datos y otros contenidos en la infraestructura de computación en la nube.

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 brinda 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 previsto en el contrato, se exige al cliente que otorgue al proveedor una licencia de uso del contenido que el cliente desee almacenar en la nube. En algunas jurisdicciones, el almacenamiento de contenido en la nube, incluso con el fin de hacer copias de seguridad, puede considerarse una reproducción y requerir la autorización previa del titular de los derechos de PI.

17. Asegurarse antes de firmar el contrato de que la utilización de los servicios de computación en la nube no supondrá una violación de derechos de PI ni una causa de revocación de la licencia concedida a cualquiera de las partes redundará en beneficio de ambas. Los costos de incurrir en una violación de derechos de PI pueden ser muy elevados. Es posible que sea necesario pactar el derecho a conceder sublicencias, o celebrar un contrato directo de licencia con el correspondiente tercero licenciante en virtud del cual se otorgue el derecho a gestionar las licencias. Para utilizar programas informáticos de código abierto u otros contenidos puede ser necesario obtener el consentimiento previo de terceros y revelar el código fuente con las modificaciones introducidas en tales programas y otros contenidos.

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

18. Como consecuencia de la migración de la totalidad o una parte de los datos a la nube, el cliente pierde tanto el control exclusivo sobre los datos como la capacidad de desplegar las medidas necesarias para garantizar la integridad y confidencialidad de estos o de verificar si los datos se están procesando y guardando correctamente. El grado de pérdida de control depende del tipo de **servicios de computación en la nube**.

19. 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**, pueden conllevar la necesidad de que las partes adopten más precauciones para evitar la interceptación de las comunicaciones y otras formas de ciberataque, que pueden 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 de recursos, la segregación de datos y unos procedimientos de seguridad sólidos son especialmente importantes cuando se trabaja en un entorno compartido como el de la computación en la nube.

20. La adopción de medidas de seguridad será una responsabilidad compartida entre las partes en el entorno de 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 relacionadas con la seguridad, la integridad, la confidencialidad y la privacidad de los datos. Las cláusulas del contrato desempeñarán un papel importante a la hora de reflejar la voluntad de las partes en cuanto a la distribución de riesgos y 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). Esas cláusulas no podrán, sin embargo, dejar sin efecto las disposiciones imperativas de la ley.

Pruebas de penetración, auditorías e inspecciones in situ

21. En la fase previa a la celebración del contrato pueden adoptarse medidas para verificar la que el aislamiento de recursos y la segregación de los datos, los

procedimientos de identificación y otras medidas de seguridad sean eficaces y suficientes. 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 prestan **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 su ubicación cumple 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 en cuanto al momento en que se realizarán, la forma en que se distribuirán sus gastos y la indemnización que deberá pagarse por los daños que eventualmente se produzcan 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, puede existir un mayor riesgo de dependencia.

24. Los riesgos de dependencia de las aplicaciones y los datos son especialmente elevados en los servicios denominados **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 para programas de aplicación, puede ser necesario volver a escribir dichos programas para tener en cuenta las interfaces 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 los servicios **IaaS**, la dependencia varía en función del tipo concreto de servicios de infraestructura utilizados, pero también puede dar lugar a una dependencia de las aplicaciones, si se depende de las características de determinadas políticas (por ejemplo, de los controles de acceso), o a una dependencia de los datos, si se traslada a la nube un mayor volumen de datos para su almacenamiento.

26. En la fase 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 reducir 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 tener otras consecuencias. Las cláusulas contractuales también pueden contribuir a mitigar los riesgos de dependencia (véase la segunda parte, en particular los párrs. 84, 85 y 143).

Riesgos de 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 fijada para la extinción del contrato, sino también cuando existe la posibilidad de una suspensión unilateral o resolución

anticipada, incluso en el supuesto 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 los efectos negativos de la cancelación o la suspensión de los servicios de computación en la nube para los usuarios finales. Algunas cláusulas contractuales también pueden ayudar a reducir los riesgos de continuidad de las operaciones (véase la segunda parte, párrs. 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 sería 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 lo que han acordado las partes acerca 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 partes en un contrato se suministren recíprocamente información que les permita tomar una decisión fundamentada sobre la celebración del contrato. La falta de una 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 dicho contrato, 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 dicha información y el propio contrato. Las partes tendrían que ocuparse también de las cuestiones relacionadas con los efectos de la información revelada en la fase precontractual en la flexibilidad y la innovación en la etapa de ejecución del contrato.

Confidencialidad

31. Es posible que parte de la información revelada en la fase anterior al contrato se considere confidencial, especialmente la relativa a las medidas de seguridad, identificación y autenticación, los subcontratistas, la ubicación de los centros de datos o la clase de centros de datos de que se trata, que puede permitir identificar el tipo de datos almacenados en ellos y las autoridades locales o de Estados extranjeros que tienen acceso a esos datos. Las partes pueden convenir en que determinada información revelada en la fase precontractual se trate de manera confidencial. Tal vez también se exija que los terceros que participen en el proceso precontractual de diligencia debida (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 suele pedirse al cliente que clasifique los datos que va a migrar, los asegure en función de su grado de importancia y confidencialidad e informe al proveedor sobre el nivel de protección necesario para cada tipo de datos. Es posible que el cliente deba también proporcionar al proveedor otro tipo de información necesaria para la prestación de los servicios (como el plan de conservación y eliminación de los datos del cliente, la identidad del usuario y los mecanismos y procedimientos de gestión de acceso para acceder a las claves de cifrado, si fuera necesario).

33. Además de la transferencia de datos y otros contenidos a la nube del proveedor, la migración a la nube puede entrañar pruebas de instalación, configuración y cifrado y la formación del personal del cliente y otros usuarios finales. Esos aspectos pueden formar parte del contrato celebrado entre el cliente y el proveedor o pueden ser objeto de un contrato independiente suscrito por el cliente con el proveedor o con 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 la migración, 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 las cláusulas no negociables aplicables a determinados tipos de contratos o las normas que penalizan el abuso del derecho o las conductas contrarias al orden público, 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 que las vincularán durante el plazo de vigencia del contrato. El derecho 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, la propuesta debe ser 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. Puede haber diferentes mecanismos de aceptación (por ejemplo, la aceptación puede consistir, en el caso del cliente, en marcar una casilla de una página web, registrarse en un servicio de computación en la nube, comenzar a utilizar los servicios de computación en la nube o pagar un precio por los servicios; 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 o en papel). Los cambios sustanciales en la oferta (por ejemplo, los referidos a la responsabilidad, la calidad y la cantidad de los servicios de computación en la nube que han de prestarse o a las condiciones de pago) pueden constituir una contraoferta que deberá ser aceptada por 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* (aquellos en que se exige la aceptación expresa previa)). En esos casos, puede haber poco o ningún margen para la negociación y modificación de la oferta estándar. Hacer clic en “Acepto”, “OK” o “De acuerdo” es el único paso necesario para celebrar el contrato. En los casos en los que se negocia el contrato, su formación puede consistir en una serie de acciones, entre las que se destacan el intercambio de información preliminar, las negociaciones, la entrega y aceptación de una oferta y la redacción 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 más documentos, como una **política de uso aceptable (PUA)**, un **acuerdo sobre la calidad y cantidad de los servicios (SLA)**, un acuerdo de procesamiento de datos o 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 el contrato conste por **escrito** (especialmente cuando incluya 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 celebrarlo **por escrito** incorporando, asimismo, todos los acuerdos complementarios, en aras de la claridad, la integridad, la exigibilidad y la eficacia del contrato y para facilitar la consulta.

40. La ley aplicable puede exigir que el contrato se firme en papel a determinados efectos, por ejemplo, por motivos fiscales, aunque este requisito es cada vez menos frecuente en el entorno sin papel.

Definiciones y terminología

41. Los contratos de computación en la nube, por la naturaleza de los **servicios de computación en la nube** que regulan, 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 el contrato, a fin de evitar ambigüedades en su interpretación. Las partes quizás podrían considerar la posibilidad de utilizar la terminología establecida internacionalmente a fin de garantizar la coherencia y la claridad jurídica.

Contenido mínimo del contrato

42. Normalmente, un contrato contiene la siguiente información: a) identificación de las partes; b) definición del objeto y el ámbito de aplicación del contrato; c) descripción de los derechos y obligaciones de las partes, incluidas las condiciones de pago; d) plazo de vigencia del contrato y condiciones de su extinción o renovación; e) medidas de reparación que podrán adoptarse en caso de incumplimiento y eximentes de responsabilidad; f) descripción de los efectos de la extinción del contrato. También es habitual incluir cláusulas de resolución de controversias, de elección de la ley aplicable y de la jurisdicción competente.

B. Identificación de las partes

43. La correcta identificación de las partes contratantes puede tener un efecto directo sobre la formación y la exigibilidad del contrato. La ley aplicable suele establecer cuál es la información necesaria para determinar si una entidad mercantil tiene personalidad jurídica y capacidad para contratar. La ley 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 obligarse en nombre de la persona jurídica.

C. Definición del objeto y ámbito de aplicación del contrato

44. El objeto de los contratos de computación en la nube varía sustancialmente en lo que se refiere a su tipología y complejidad, dado que existe una diversa gama de **servicios de computación en la nube**. Dentro del período de vigencia de un contrato su objeto puede variar: es posible que se cancelen algunos **servicios de computación en la nube** y que se añadan otros. El objeto del contrato puede abarcar la prestación de servicios esenciales, auxiliares y opcionales.

45. En la descripción del objeto del contrato se suele incluir una descripción del tipo de servicios de computación en la nube (**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 forman el contrato pueden resultar pertinentes a la hora de determinar su objeto (véase el párr. 38 *supra*).

Acuerdo sobre la cantidad y calidad de los servicios

46. En el **acuerdo sobre la cantidad y calidad de los 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 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. Es posible que en esos planes se prevea el tiempo máximo de resolución de 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 y protección de los datos. Algunos aspectos del servicio pueden medirse tanto en función de parámetros cualitativos como 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 y la calidad y la seguridad de las medidas que pueda ser necesario adaptar según los distintos grados de confidencialidad 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 estos parámetros cuantitativos, o en lugar de ellos, el cifrado puede medirse utilizando un parámetro cualitativo (por ejemplo, el proveedor debe asegurarse de que los datos del cliente estén cifrados cuando se transporten por una red de comunicaciones pública, así como cuando estén en reposo en los centros de datos del proveedor).

49. Podrían pactarse distintos tipos de obligaciones (es decir, obligaciones de resultado u obligaciones 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 estipulara 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 obligaciones 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 prestan o en el momento en que se utilizan los servicios). 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 medir o verificar las mediciones realizadas por el proveedor o por terceros, pero solo de las que evalúen los servicios en el momento en que se utilizan, no en el momento en que se prestan. El cliente tal vez pueda evaluar 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, o en forma periódica (diaria, semanal, mensual, etc.) o cuando se produzca un determinado incidente. Como alternativa a lo anterior, el proveedor puede conceder al cliente el derecho a revisar sus registros de las evaluaciones de la cantidad y calidad 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 exigir que alguna de las partes o ambas conserven durante un tiempo determinado 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. Una **política de uso aceptable (PUA)** fija las condiciones de uso por parte del 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 con el proveedor. La inmensa mayoría de las **PUA** estándar prohíben un conjunto similar de 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 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 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 la respeten. Algunos proveedores pueden exigir que los clientes impidan proactivamente todo uso no autorizado o inadecuado por parte de terceros de los servicios de computación en la nube que 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 y no autorice ni permita deliberadamente tales usos, y que notifique al proveedor todo uso no autorizado o inadecuado del que tenga conocimiento.

55. En algunas jurisdicciones, la ley podría imponer obligaciones a los proveedores en relación con el contenido alojado en su infraestructura de computación en la nube, por ejemplo, la obligación de informar a las autoridades públicas de la existencia de material ilegal. Es posible que no se permita trasladar esas obligaciones al cliente ni a los usuarios finales mediante la **PUA** ni por otras vías. Podrían tener ramificaciones relacionadas con la privacidad y de otra índole y serían uno de los factores a tener en cuenta a la hora de 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. Se debería especificar en el contrato las funciones y las responsabilidades de cada parte en lo que respecta a las medidas de seguridad, para reflejar las obligaciones impuestas a alguna de las partes o a ambas por normas legales imperativas.

57. Por lo general, el proveedor aplica sus propias políticas de seguridad. En algunas situaciones podría llegar a convenirse en que el proveedor aceptase las políticas de seguridad del cliente, aunque no en el caso de las **soluciones de nube genéricas y estandarizadas para múltiples suscriptores**. En el contrato pueden detallarse las medidas de seguridad que han de adoptarse (por ejemplo, los requisitos para la eliminación, irreversible o no, de los datos almacenados en un soporte dañado, el almacenamiento de distintos paquetes de datos en diferentes ubicaciones o el almacenamiento de los datos del cliente en un equipo físico concreto exclusivo para ese cliente). No obstante, incluir una cantidad excesiva de información de seguridad en el contrato puede ser 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 que realiza el proveedor respecto del equipo físico en el que se almacenan los datos y se ejecutan los servicios, así como las medidas eficaces para controlar el acceso a dichos equipos. En otros casos, el hecho de permitir que una de las partes cumpla sus deberes o evalúe y controle la calidad de las medidas de seguridad adoptadas puede hacer necesaria la actuación de la otra parte. El cliente podría estar obligado, por

ejemplo, a actualizar las listas con las credenciales de los usuarios y sus derechos de acceso, e informar de los cambios al proveedor con la antelación suficiente para garantizar el correcto funcionamiento de los mecanismos de gestión de la identidad y acceso. El cliente también podría tener que comunicar al proveedor el nivel de seguridad que debe aplicarse 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 quizás hagan necesario que las condiciones del contrato de computación en la nube se armonicen con 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 instancia, 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, es posible que el cliente se plantee si será necesario garantizar el acceso a por lo menos una de las copias utilizables de sus datos que se encuentren fuera del control, el alcance o la influencia del proveedor y sus subcontratistas y en la que estos no tengan participación.

Cláusula de confidencialidad

62. La voluntad del proveedor de comprometerse a garantizar la confidencialidad de los datos del cliente dependerá de la naturaleza de los servicios que hayan de prestarse a este con arreglo al contrato y, en especial, de si es necesario que el proveedor tenga 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 rechacen expresamente 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 durante las negociaciones contractuales, pero no la de los datos procesados durante la prestación de los servicios. Algunas de las cláusulas de confidencialidad estándar propuestas por los proveedores pueden no ser suficientes para garantizar el cumplimiento de la legislación aplicable.

63. En ausencia de compromisos contractuales y requisitos legales que obliguen al proveedor a mantener la confidencialidad, toda la responsabilidad de proteger el carácter reservado de los datos, por ejemplo mediante el cifrado de los datos, recaerá sobre el cliente. Cuando no exista la posibilidad de 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 (con un régimen de responsabilidad diferente para el incumplimiento de la obligación de confidencialidad impuesta en relación con dichos datos). Al cliente pueden preocuparle especialmente sus secretos comerciales, sus conocimientos especializados y aquella información que sea necesario mantener en secreto por disposición legal o debido a compromisos asumidos con terceros. Las partes pueden convenir en restringir el acceso a esos datos a un número limitado de personas y exigir a esas personas que asuman compromisos individuales 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 detección de intrusos y de responder a incidentes). En esos casos, normalmente correspondería al cliente especificar al proveedor la información confidencial, el nivel de protección necesario, la legislación aplicable o los requisitos contractuales y todos los cambios que afecten a esa información, entre ellos los cambios 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 estar impuesta en la ley, por ejemplo, cuando existe el deber de aportar información a las autoridades estatales 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 ni otros detalles de los servicios que este presta al cliente conforme a su contrato o a lo previsto en la ley.

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

66. Los **datos personales** son objeto de una protección legal especial en muchas jurisdicciones. La legislación 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. El contrato puede incluir 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, su objeto, su 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 existe la posibilidad de 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 dan garantías suficientes de que el **procesamiento de los datos personales** se realizará de acuerdo con la ley y si prevén mecanismos adecuados de reparación 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 la legislación 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, incluidas las peticiones relativas a los **derechos de los sujetos de los datos**. Las partes quizás pacten también, por separado, medidas de reparación para el caso de que se incumplan esas cláusulas, entre ellas la rescisión unilateral del contrato y 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 el proveedor actúe como **procesador de los datos** solamente cuando procese los datos del cliente siguiendo sus instrucciones con el único fin de prestar los servicios de computación en la nube. No obstante, y con independencia de lo pactado en el contrato, en algunas jurisdicciones el proveedor puede ser considerado el **responsable de los datos** cuando además procese los datos para sus propios fines o siguiendo las instrucciones de las autoridades del Estado, en cuyo caso podría tener que asumir la plena responsabilidad de la protección de los **datos personales** que fuesen objeto de ese **procesamiento de datos personales** ulterior (véase el párr. 125 *infra*).

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

70. Tanto la ley como el contrato, o ambos, pueden obligar a las partes a que se notifiquen mutuamente y de inmediato los **incidentes de seguridad** de importancia para el contrato que se produzcan o cualquier sospecha que tengan de que se haya producido un incidente. Esa obligación puede existir con independencia de la obligación general establecida en la ley de notificar los incidentes de seguridad que se produzcan a todas las partes interesadas, incluidos los **sujetos de los datos**, las compañías de seguros, las autoridades del Estado o el público en general, a fin de evitar o reducir al mínimo los efectos de esos incidentes.

71. Es posible que la ley especifique determinados requisitos de notificación de incidentes de seguridad, entre ellos el momento en que se debe realizar la notificación, y que indique quiénes son los responsables de que se cumplan esos requisitos. Siempre y cuando se atengan a esas disposiciones obligatorias, las partes pueden especificar en el contrato el plazo de notificación (por ejemplo, un día después de que la parte haya tenido conocimiento del incidente o la amenaza) y la forma y el contenido de la notificación del incidente de seguridad. En cuanto al contenido, este suele incluir 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. Puede incluir también información sobre intentos fallidos de quebrantar la seguridad, ataques contra objetivos concretos (por cada usuario del cliente, por cada aplicación específica, por cada máquina física concreta), tendencias y estadísticas. Los requisitos de notificación suelen tener en cuenta la necesidad de no revelar información confidencial que pudiera poner en riesgo los sistemas, la red o las operaciones de la parte afectada.

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"), como 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. El informe de análisis del incidente puede ser realizado por el afectado, o por este juntamente 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 rescisión del contrato.

Requisitos de ubicación de los datos

74. El proveedor, en sus condiciones estándar, puede reservarse expresamente el derecho de alojar los datos del cliente en cualquier país en el 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 es algo implícito en la prestación de los **servicios de computación en la nube** que, por regla general, se suministran desde más de un lugar (por ejemplo, las copias de seguridad y la protección antivirus pueden hacerse a distancia y el servicio de apoyo al cliente puede ofrecerse siguiendo el modelo de **aprovechamiento de los husos horarios**). Esa práctica puede no cumplir 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. Pueden incluirse en el contrato medidas de salvaguardia destinadas a garantizar el cumplimiento de los **requisitos de ubicación de los datos**, como la prohibición de trasladar los datos y otros contenidos fuera de la ubicación especificada 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, los **metadatos** y sus copias de seguridad) se almacenen exclusivamente en centros de datos ubicados físicamente en las jurisdicciones indicadas en el contrato y cuya propiedad y administración corresponda a entidades establecidas en tales jurisdicciones. Como alternativa a lo anterior, el parámetro podría, por ejemplo, prohibir que los datos se trasladaran fuera de un país o región concretos, pero permitir que se duplicaran en un determinado país o en otros países, aunque nunca en un país concreto.

D. Derechos a los datos y otros contenidos del cliente

Derechos del proveedor a acceder a los datos del cliente para prestar los servicios

76. Los proveedores suelen reservarse el derecho de acceder a los datos del cliente siempre y cuando "necesiten conocerlos". Esto permite que los empleados y

subcontratistas del proveedor, y otros terceros (por ejemplo, los auditores), tengan acceso a los datos del cliente cuando sea necesario para la prestación de los servicios de computación en la nube (con fines de mantenimiento, apoyo y seguridad, entre otros) y para supervisar el cumplimiento de lo establecido en la **PUA**, las **licencias de PI**, el **SLA** y otros documentos contractuales. Las partes pueden pactar las situaciones en que se permitirá el acceso del proveedor a los datos del cliente y las medidas que se adoptarán para garantizar la confidencialidad y la integridad de dichos datos.

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

78. En el contrato puede indicarse expresamente cuáles son los derechos necesarios para el cumplimiento del contrato que el cliente otorga al proveedor respecto de los datos; si el proveedor puede, y en qué medida, transferir esos derechos a terceros (por ejemplo, a sus subcontratistas), y cuál es el ámbito geográfico y temporal de los derechos concedidos expresa o implícitamente. Las limitaciones geográficas podrían ser especialmente importantes en los casos en que la ley prohíbe que los datos salgan de un determinado país o región (véase la primera parte, párrs. 10 y 11). Los contratos suelen indicar si el cliente tiene o no la facultad de revocar los derechos otorgados expresa o implícitamente y, en caso afirmativo, en qué condiciones. Dado que la capacidad de prestar los servicios con el nivel de calidad exigido puede depender de los derechos otorgados por el cliente, la revocación de determinados derechos puede tener como consecuencia directa la modificación o rescisión del contrato.

Utilización de los datos del cliente por el proveedor 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 tales casos, las preguntas que cabe formular son, entre otras: a) qué información sobre el cliente y sus usuarios finales se recopilará y por qué motivos y con qué fines el proveedor la recopilará y utilizará; b) si esa información se va a compartir con otras organizaciones, empresas o particulares y, de ser así, por qué motivo y si esto se hará con o sin el consentimiento del cliente; y c) de qué manera se va a garantizar el cumplimiento de las políticas de confidencialidad y seguridad si el proveedor comparte esa información con terceros. Además, en los casos en que la utilización por el proveedor de los datos del cliente afecte a **datos personales**, normalmente se supone que las partes evaluarán cuidadosamente sus respectivas obligaciones de cumplir lo previsto 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 las circunstancias en que se permitirá dicho uso, se establezca la obligación de anonimizar los datos del cliente u ocultar su identidad a fin de garantizar el cumplimiento de la normativa aplicable en materia de protección de datos y otras normas, e imponer límites a la reproducción del contenido y a la 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 posteriormente, pero como datos abiertos y anónimos o de forma agregada y sin que se identifique al cliente.

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

81. Las condiciones estándar de los proveedores pueden conceder a estos el derecho a utilizar los nombres, logotipos y marcas del cliente en su propia publicidad. Las partes pueden convenir en suprimir o modificar esas disposiciones, por ejemplo, limitando el uso permitido del nombre del cliente y exigiendo que se obtenga la autorización previa de este para poder utilizar su nombre, su logotipo y su marca.

Medidas adoptadas por el proveedor con respecto a los datos del cliente tras recibir una orden del Estado o para cumplir la normativa vigente

82. En sus condiciones estándar, el proveedor puede reservarse el derecho a revelar, a su entera discreción, los datos del cliente, o a proporcionar acceso a estos a las autoridades del Estado (por ejemplo, incluyendo una frase de un tenor similar al siguiente: "cuando hacerlo sea en el interés superior del proveedor"). En las condiciones del proveedor también se suele contemplar el derecho de este a retirar o bloquear los datos del cliente inmediatamente después de tener conocimiento de la existencia de contenido ilícito o cuando tiene que hacer respetar el **derecho al olvido** de **los sujetos de los datos** para no incurrir en responsabilidad legal (el procedimiento de "notificación y retirada" (véase el párr. 128 *infra*)). Las partes pueden convenir en limitar los supuestos en que el proveedor estará autorizado a actuar de ese modo, como cuando reciba una orden de un tribunal u otra autoridad del Estado instándole a facilitar el acceso a los datos, a suprimirlos o a modificarlos.

83. Las partes pueden acordar, como mínimo, que se notifiquen de inmediato al cliente las órdenes del Estado o las propias decisiones del proveedor en lo que respecta a los datos del cliente, incluyendo 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, el contrato puede exigir que el proveedor notifique esa misma información al cliente inmediatamente después. Las partes podrán incluir también disposiciones que obliguen a llevar un registro de todas las órdenes, solicitudes y demás actividades relacionadas con los datos del cliente, y conceder a este último acceso a ese registro.

Derechos a los datos obtenidos de los servicios de nube

84. Las partes pueden pactar los derechos que tendrá el cliente a los **datos obtenidos de los servicios de nube** y la forma en que podrán ejercerse esos derechos durante la 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 hacer nacer objetos de derechos de PI, ya sea conjuntamente para el proveedor y el cliente (por ejemplo, las mejoras de los servicios derivadas de las sugerencias del cliente) o solo para el cliente (nuevas aplicaciones, programas informáticos y otros productos originales). El contrato puede incluir una cláusula expresa sobre PI que determine a cuál de las partes en el contrato pertenecen los derechos de PI sobre los objetos desplegados o desarrollados en la nube, y cómo pueden las partes usarlos. Cuando no exista la posibilidad de negociar este aspecto, el cliente tal vez desee revisar las cláusulas de PI a fin de determinar si el proveedor le ofrece suficientes garantías y le permite disponer de los instrumentos necesarios para proteger y ejercitar sus derechos de PI, evitando 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**. A menos que en el contrato se disponga otra cosa, podría recaer enteramente sobre el cliente la carga de crear procedimientos compatibles de exportación de datos, por ejemplo, mediante la inclusión de compromisos contractuales en lo que respecta a la interoperabilidad, la portabilidad y la asistencia para exportar los datos en el momento en que se extinga el contrato (véase el

párr. 161 *infra*). El contrato puede exigir el uso de formatos de exportación de datos y otros contenidos interoperables o estandarizados que sean comunes y ampliamente utilizados, o dar derecho a elegir entre diferentes formatos. También pueden incluirse en el contrato cláusulas que contemplen el derecho a utilizar productos y aplicaciones o programas informáticos conjuntos sin los cuales sería 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 se exija que los clientes puedan buscar y encontrar datos alojados en la nube en su formato original con una finalidad jurídica, por ejemplo, en el marco de una investigación. Tal vez sea necesario que los registros electrónicos cumplan las normas de auditoría y los requisitos exigidos en materia de prueba. Algunos proveedores quizás estén en condiciones de ofrecer asistencia a los clientes para recuperar los datos en el formato exigido por la ley. El contrato puede establecer la forma y las condiciones de dicha asistencia.

Eliminación de datos

88. La **eliminación de datos** es una cuestión que puede plantearse durante toda la 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. Los datos de carácter delicado pueden tener que ser destruidos en un momento determinado de su ciclo de vida (por ejemplo, mediante la destrucción de los discos duros al finalizar la vida útil del equipo en que se almacenaban esos datos). También puede ser necesario eliminar los datos para cumplir un mandamiento legal de eliminación o cuando se confirme que se han vulnerado derechos de PI (véase el párr. 82 *supra*).

89. Es posible que en las cláusulas estándar del proveedor se establezca únicamente que los datos del cliente se eliminarán cada cierto tiempo. Las partes pueden pactar que los datos, sus copias de seguridad y los **metadatos** se eliminarán de manera inmediata, eficaz, irrevocable y permanente, de conformidad con el calendario de conservación y eliminación de datos u otras autorizaciones o solicitudes comunicadas por el cliente al proveedor. El contrato puede establecer el plazo y otras condiciones para 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 exija la aplicación de determinadas normas o técnicas de eliminación. Puede exigirse la eliminación de datos en distintos lugares y soportes, incluidos los sistemas de los subcontratistas y otros terceros, y en diverso grado, por ejemplo, desde una eliminación de los datos que asegure su confidencialidad, hasta su completa eliminación o la destrucción del equipo físico. Existen otros procedimientos de eliminación más seguros que conllevan la destrucción en lugar de la redistribución del equipo, pero pueden resultar más costosos y no siempre es posible llevarlos a cabo (si, por ejemplo, hay datos de otras personas almacenados en el mismo equipo). Estos aspectos pueden dar lugar a que se establezcan en el contrato requisitos como la utilización de 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 el contrato y se respete la normativa aplicable (por ejemplo, verificando que el cliente y sus usuarios finales respetan la **PUA** y las **licencias de PI**, y que el proveedor actúe de conformidad con el **SLA** y la política de protección de los

datos). Algunas actividades de supervisión, como las relacionadas con el **procesamiento de datos personales**, pueden ser obligatorias por disposición de la ley.

92. El contrato puede establecer actividades de supervisión periódicas o recurrentes, indicando qué parte será responsable de su ejecución y obligando a la otra parte a facilitar la supervisión. También se pueden prever en el contrato actividades excepcionales de supervisión, ofreciendo opciones para su gestión, así como la obligación de notificar a la otra parte y los compromisos de confidencialidad relacionados con tales actividades de supervisión.

93. Una supervisión excesiva puede afectar a la calidad o la cantidad de los servicios y aumentar el costo de estos. El contrato puede establecer la obligación de suspender la supervisión en determinados casos, por ejemplo, cuando esta suponga un perjuicio importante para la calidad o la calidad de los servicios. Esa circunstancia puede darse principalmente en el caso de los servicios que deben prestarse casi en tiempo real.

Auditorías y pruebas de seguridad

94. Las auditorías y las pruebas de seguridad son bastante comunes, en especial las destinadas a comprobar la eficacia de las medidas de seguridad. Algunas auditorías y pruebas de seguridad pueden ser obligatorias por disposición de la ley. El contrato puede contener cláusulas que definan los derechos de ambas partes en materia de auditoría y reglamenten el alcance, la frecuencia, las formalidades y los gastos de las auditorías. También puede obligar a las partes a que se comuniquen mutuamente los resultados de las auditorías o las pruebas de seguridad encargadas por cada una de ellas. Es posible que tanto los derechos contractuales como las obligaciones legales relacionadas con la auditoría y las pruebas de seguridad deban complementarse en el contrato con las obligaciones respectivas de la otra parte de facilitar el ejercicio de esos derechos o el cumplimiento de esas obligaciones (permitiendo, por ejemplo, el acceso a los centros de datos pertinentes).

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

F. Condiciones de pago

Pago por uso

96. El precio es un elemento esencial del contrato. Cuando este no fija el precio o un mecanismo que permita determinarlo, puede llegar a ser imposible exigir el cumplimiento de ese contrato.

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

Derechos de licencia

98. Es posible que las partes deseen aclarar en el contrato si el pago de los servicios de computación en la nube incluye los derechos de licencia correspondientes a las licencias que el proveedor pueda conceder al cliente como parte de los servicios. Los servicios **SaaS**, en especial, suelen conllevar la utilización por parte del cliente de programas informáticos con licencia del proveedor.

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 diversas formas de pago pueden tener consecuencias diferentes. Por ejemplo, el costo de una licencia para un cliente puede aumentar de manera exponencial si los programas informáticos se cobran por instancia cada vez que se conecta una máquina nueva, aun cuando el cliente esté utilizando el mismo número de instancias durante el mismo período.

100. El contrato puede fijar el número total de posibles usuarios de un programa informático que estarán amparados por el acuerdo de licencia, el número de usuarios de cada categoría (por ejemplo, empleados, contratistas independientes y proveedores) y los derechos que se concederán a cada una de ellas. El contrato también puede establecer 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, por consiguiente, a que aumente el importe de los derechos que deberán pagarse por ella.

Gastos adicionales

101. El precio puede abarcar también algunos gastos puntuales (por ejemplo, la configuración y la migración a la nube; véase la primera parte, párrs. 32 y 33). 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, facturando esos servicios por tiempo o por un precio fijo).

102. La inclusión o no de los servicios de computación en la nube en la categoría de servicios o bienes imponibles dependerá de cada jurisdicción. 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 (como la facturación electrónica) y la forma y el contenido de las facturas, aspecto que puede resultar importante a los efectos de cumplir las normas tributarias. Es posible que los organismos tributarios de algunas jurisdicciones no acepten facturas electrónicas (aunque esto es cada vez más infrecuente en los entornos en que no se utiliza el papel) o exijan 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 otras condiciones, la fecha de pago, la moneda, el tipo de cambio aplicable, la forma de realizar el pago, las sanciones en caso de retrasos en los pagos y los procedimientos para resolver las controversias relativas a reclamaciones de pago.

G. Cambios en los servicios

105. Los **servicios de computación en la nube** son, por naturaleza, flexibles y fluctuantes. Las características de **elasticidad, escalabilidad** y **autoservicio a pedido** de los **servicios de computación en la nube** suelen ofrecerse al cliente mediante varias opciones incluidas en el contrato que el cliente puede utilizar para adaptar el consumo de los servicios a sus necesidades. Con ello se evita la necesidad de renegociar 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. El tratamiento contractual apropiado en cada caso puede ser diferente en función de si los cambios se refieren a los servicios principales o a servicios auxiliares y cuestiones de apoyo. También es posible que se aplique un tratamiento diferente a los cambios que puedan afectar negativamente a los servicios y a aquellos que puedan suponer mejoras (por ejemplo, el paso de una oferta estándar de servicios de computación en la nube a una oferta mejorada con mayores niveles de seguridad o menores tiempos de respuesta). Algunos cambios realizados unilateralmente por el proveedor en las condiciones estipuladas en el contrato pueden tener graves consecuencias para el cliente, en particular cuando los cambios dan lugar a gastos elevados de migración a otro sistema.

Cambios en los precios

107. El proveedor puede reservarse el derecho a modificar unilateralmente el precio o las escalas de precios. Las partes pueden convenir en pactar en el contrato la metodología de fijación de precios (por ejemplo, con qué frecuencia y en qué medida el proveedor puede aumentar los precios). El aumento de los precios puede limitarse, utilizando para el cálculo del precio máximo un determinado índice de precios de consumo, un porcentaje fijo o el listado de precios del proveedor vigente en un momento dado. El contrato puede obligar a que se notifique con antelación el aumento de precios y detallar las consecuencias de que el cliente no acepte ese aumento.

Actualizaciones

108. Si bien las actualizaciones pueden ser en interés del cliente, también pueden causar trastornos en la disponibilidad de los servicios de computación en la nube, ya que podrían conllevar **períodos de interrupción o corte del servicio** relativamente prolongados durante el horario normal de funcionamiento, aun cuando se trate de un servicio prestado en forma ininterrumpida. Las partes pueden pactar la obligación de notificar al cliente con antelación las actualizaciones pendientes y sus consecuencias, y 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 deben emplearse para comunicar y resolver posibles problemas.

109. Es posible que las actualizaciones tengan otros efectos negativos, como la necesidad de hacer cambios en las aplicaciones o los sistemas informáticos del cliente o de capacitar nuevamente a los usuarios de este. El contrato puede prever el reparto de los gastos derivados de las actualizaciones. Cuando se vayan a realizar cambios importantes en la versión anterior del servicio prestado, las partes pueden acordar también que se mantenga dicha versión en paralelo con la nueva durante un plazo convenido, a fin de garantizar la continuidad de las operaciones del cliente. En el contrato se puede prever también la cuestión de la asistencia que ofrecerá el proveedor cuando se realicen cambios en las aplicaciones o los sistemas informáticos del cliente y para impartir nueva capacitación a los usuarios finales del cliente, si fuera necesario.

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, dando por finalizada una parte de estos. Sin embargo, la interrupción incluso de algunos servicios de computación en la nube por parte del proveedor puede hacer incurrir en responsabilidad al cliente frente a sus usuarios finales.

111. Es posible que el contrato establezca la obligación de enviar al cliente una notificación previa de esos cambios, el derecho de este último a rescindir el 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. Algunos contratos prohíben las modificaciones que podrían afectar de forma negativa a la naturaleza, el alcance o la calidad de los servicios prestados,

o limitan los cambios permitidos a “modificaciones razonables desde el punto de vista comercial”.

Notificación de los cambios

112. En las condiciones estándar de los proveedores puede establecerse la obligación del proveedor de notificar al cliente los cambios en las condiciones de los servicios. De no ser así, es posible que se pida a los clientes que comprueben regularmente si se han producido cambios en el contrato. Los documentos que integran el contrato pueden ser numerosos (véase el párr. 38 *supra*). Algunos pueden incorporar por remisión condiciones y políticas establecidas en otros documentos, los que a su vez quizás incorporen por remisión otras condiciones y políticas, que pueden, todas ellas, ser objeto de modificación unilateral por parte del proveedor. Esos distintos documentos no tienen que estar necesariamente almacenados en un único lugar del sitio web del proveedor. En consecuencia, los cambios introducidos por el proveedor en el contrato tal vez no sean fáciles de advertir.

113. Dado que la utilización continuada de los servicios por parte del cliente se considera una aceptación de las nuevas condiciones, las partes pueden convenir en que se notifique al cliente los cambios que se realicen en las condiciones de los servicios con suficiente antelación antes de su fecha de 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. Las condiciones estándar de los proveedores pueden contemplar el derecho de estos a suspender los servicios a su entera discreción en cualquier momento. La expresión “acontecimientos imprevisibles” se utiliza habitualmente para justificar la suspensión unilateral de los servicios por parte del proveedor. Esos acontecimientos suelen definirse de una manera amplia para abarcar cualquier impedimento que esté fuera del control del proveedor, incluido el incumplimiento de los subcontratistas, los proveedores del proveedor y otros terceros que participan en la prestación de los servicios de computación en la nube a los clientes, tales como los proveedores de acceso a Internet.

115. Las partes pueden pactar que la suspensión de los servicios esté permitida solamente en unos pocos casos definidos en el contrato (por ejemplo, si el cliente incurre en un incumplimiento esencial del contrato, como la falta de pago). El derecho de suspensión a causa de acontecimientos imprevisibles puede estar sometido a la condición de que se ponga debidamente en marcha un plan de recuperación en casos de desastre y continuidad de las operaciones. El contrato puede disponer que ese plan incluya medidas de protección frente a los peligros más comunes a que está expuesta la prestación de los servicios de computación en la nube y que le sea enviado a la otra parte para su consideración y aprobación. Entre esas medidas de protección pueden figurar la existencia de un sitio de recuperación geográficamente independiente al que pueda pasarse sin problemas en caso de desastre y la utilización de fuentes de energía eléctrica ininterrumpida 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 comunes en el entorno de la computación en la nube. En las condiciones estándar de los proveedores, estos pueden reservarse expresamente el derecho a recurrir a terceros para prestar al cliente los servicios de computación en la nube, o ese derecho puede resultar 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. La ley puede exigir a las partes que indiquen en el contrato a los terceros que participarán en la prestación de los servicios de computación en la nube. La identificación de esos terceros puede representar una ventaja para el cliente, al permitirle verificar información, especialmente en lo que respecta al cumplimiento por parte de esos terceros de los requisitos de seguridad, confidencialidad, protección de datos y otros requisitos establecidos en el contrato o en la ley, así como verificar la inexistencia de conflictos de intereses de dichos terceros.

118. Esa información puede utilizarse también para reducir el riesgo de incumplimiento del contrato por el proveedor debido a los incumplimientos 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 puede también tratar de negociar con los terceros clave la obligación de estos de intervenir en caso de que el proveedor no cumpla lo previsto en el contrato, incluso en caso de insolvencia del proveedor.

119. El proveedor quizás pueda indicar quiénes son los terceros que desempeñan papeles fundamentales, si bien no siempre podrá identificar a todos los terceros. El conjunto de los terceros que intervienen en la prestación de los servicios de computación en la nube puede cambiar durante el contrato (véanse los párrs. 120 y 121 *infra*).

Cambios en la cadena de subcontratación

120. Los cambios unilaterales en la cadena de subcontratación son algo habitual. El contrato puede especificar si se permiten o no los cambios en la cadena de subcontratación y, en caso afirmativo, en qué condiciones pueden realizarse. Por ejemplo, el cliente puede reservarse el derecho a investigar los antecedentes de cualquier tercero que se quiera hacer participar en la prestación de los servicios de computación en la nube y vetarlo antes de que se realice el cambio. Como alternativa a lo anterior, puede incluirse en el contrato una lista de terceros previamente aprobados por el cliente, entre los cuales el proveedor podrá elegir cuando sea necesario. Otra opción consiste en someter el cambio a su posterior aprobación por parte del cliente y, de no concederse esa aprobación, los servicios tendrían que continuar prestándose con el anterior tercero, con otros terceros previamente aprobados o con algún otro que las partes designaran de común acuerdo. De lo contrario, el contrato podría rescindirse.

121. Las disposiciones imperativas de la ley aplicable pueden establecer en qué circunstancias los cambios en la cadena de subcontratación del proveedor pueden dar lugar a la rescisión del contrato.

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

122. La ley o el contrato pueden exigir a las partes que armonicen las condiciones de este último con las de otros contratos vigentes o futuros vinculados al primero a fin de asegurar la confidencialidad y el cumplimiento de los requisitos de **ubicación de los datos** y protección de los datos. El contrato puede obligar a las partes a que se entreguen mutuamente copias de los contratos vinculados con fines de verificación.

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

123. Si bien es posible incluir en el propio contrato de computación en la nube una lista de los terceros que sean imprescindibles para la ejecución del contrato, estos no serán partes en el contrato celebrado entre el proveedor y el cliente. Solo responderán de las obligaciones asumidas en virtud de su contrato 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 incumpliera el contrato vinculado.

124. Con arreglo a lo previsto en la ley aplicable o en el contrato, el proveedor puede incurrir en responsabilidad frente al cliente por cualquier cuestión encomendada a un tercero que el proveedor haya hecho participar en la ejecución del contrato. En concreto, la ley puede establecer la responsabilidad conjunta del proveedor y sus subcontratistas respecto de las cuestiones que pudieran plantearse en materia de **procesamiento de datos personales**, según el grado de participación de los subcontratistas en el procesamiento de datos.

J. Responsabilidad

Restricciones legales a la libertad contractual

125. Si bien la mayoría de los ordenamientos jurídicos reconocen en general el derecho de las partes contratantes a distribuir los riesgos y las responsabilidades y a limitar o excluir su responsabilidad mediante disposiciones del contrato, ese derecho suele estar sujeto a ciertos límites y condiciones. Por ejemplo, en lo que respecta al **procesamiento de datos personales**, un factor importante en la distribución de riesgos y responsabilidades es la función que cada parte asume en relación con los **datos personales** alojados en la nube. La legislación sobre protección de datos de determinadas jurisdicciones impone una responsabilidad mayor al **responsable de los datos** que al **procesador de los datos personales**. A pesar de lo que disponga el contrato, el manejo efectivo de esos datos será lo que normalmente determine el régimen legal a que estará sometida una parte con arreglo al derecho aplicable. Los **sujetos de datos** que hayan sufrido pérdidas como consecuencia del procesamiento ilícito 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 derivada de la propia culpa no es admisible, o se permite con limitaciones. Tal vez no sea posible excluir en su conjunto la responsabilidad por lesiones (incluidas la enfermedad y el fallecimiento) 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 la exoneración de responsabilidad del proveedor por **incidentes de seguridad** en los casos en que el cliente no tenga el control de las medidas de seguridad ni la capacidad de adoptarlas, pueden considerarse “abusivas” y, por tanto, nulas. Las condiciones de los contratos de adhesión, que no suelen negociarse sino que vienen preestablecidas por una de las partes, pueden ser objeto de un examen particularmente minucioso. Además, en el caso de algunos tipos de vicios (por ejemplo, defectos en los equipos físicos o los programas informáticos), la ley puede establecer la responsabilidad ilimitada.

127. Las instituciones públicas pueden ver limitada por ley su capacidad de asumir determinadas responsabilidades, o pueden necesitar la autorización previa de un órgano estatal competente para poder hacerlo. También pueden tener 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 cumpliera determinados criterios que, de no satisfacerse, podrían hacer incurrir a esa parte en responsabilidad. Por ejemplo, según el procedimiento de “detección y retirada” vigente en algunas jurisdicciones, el proveedor quedará liberado de responsabilidad por alojar contenido ilegal en su infraestructura de nube si retira dicho contenido una vez tenga conocimiento de su ilegalidad.

129. Algunas jurisdicciones exigen que las cláusulas que contienen descargos y limitaciones de responsabilidad pactados por las partes figuren en el contrato para que sean exigibles. La ley aplicable podría imponer requisitos de forma o de otra índole para la validez y exigibilidad de esas cláusulas.

Otras cuestiones a tener en cuenta a la hora de redactar cláusulas de responsabilidad

130. En el momento de negociar la distribución de los riesgos y las responsabilidades deberían tenerse en cuenta el importe cobrado, en su caso, por los servicios de computación en la nube y los riesgos inherentes a la prestación de los servicios. Aunque las partes tienden por lo general a excluir o limitar la responsabilidad derivada de los factores que no pueden controlar 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. Las partes pueden estar dispuestas a asumir riesgos y responsabilidades por elementos que no pueden controlar con el fin de distinguirse en el mercado. Sin embargo, es más probable que los riesgos y las responsabilidades de las partes aumenten progresivamente en forma proporcional a los elementos que estén bajo su control.

131. Por ejemplo, en los servicios **SaaS** en que se utilizan tipos estándar de programas informáticos de oficina, 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 no haber realizado las copias de seguridad necesarias podría dar lugar a la pérdida del derecho a reclamar contra el proveedor en caso de pérdida de los datos. Por otro lado, en el caso de los servicios **IaaS** y **PaaS**, el proveedor podría incurrir en responsabilidad únicamente con respecto a la infraestructura o las plataformas proporcionadas (como los equipos físicos, los sistemas operativos o los programas intermedios), mientras que el cliente tendría que responder de todos los componentes que le pertenecieran, como las aplicaciones utilizadas en la infraestructura o las plataformas del proveedor y los datos alojados en ellas.

Condiciones estándar del proveedor

132. Las condiciones estándar de los proveedores pueden excluir toda responsabilidad contractual y plegarse a la tesis de que las cláusulas de responsabilidad son innegociables. Otra posibilidad es que el proveedor esté dispuesto a aceptar su responsabilidad, incluso una responsabilidad ilimitada, por las infracciones que estén bajo su control (por ejemplo, una violación de las licencias de PI concedidas por el cliente al proveedor), pero que no se haga responsable de las infracciones que puedan derivarse de hechos que escapen a su control (como los acontecimientos imprevisibles o 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 derivados (por ejemplo, la pérdida de oportunidades comerciales a raíz de la falta de disponibilidad de los servicios de computación en la nube). Cuando se acepta asumir responsabilidad de una forma general o en determinados casos, las condiciones estándar de los proveedores suelen limitar la cuantía de los daños por los que se responderá (por siniestro, por serie de siniestros relacionados entre sí o por períodos de tiempo). Además, los proveedores suelen fijar un límite máximo general a la responsabilidad contractual, que puede estar vinculado a los ingresos que se espera obtener del contrato, a la facturación del proveedor o a la cobertura del seguro.

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 acontecimientos (por ejemplo, la transgresión de las políticas de protección de datos personales y la violación de los derechos de PI) podrían exponer a cualquiera de las partes a un nivel posiblemente alto de responsabilidad frente a terceros o dar lugar a la imposición de multas reglamentarias. Es frecuente, por tanto, que se pacte un régimen de responsabilidad más severo (responsabilidad ilimitada

o indemnizaciones más elevadas) cuando las infracciones sean imputables a la culpa o negligencia de la otra parte.

136. Por otra parte, la responsabilidad de las partes por las acciones de terceros que escapen a su control (por ejemplo, la responsabilidad del cliente por el comportamiento de los usuarios finales, o del proveedor por las acciones del cliente o sus usuarios finales) puede estar limitada o excluida por el contrato o por la ley.

Seguro de responsabilidad civil

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

K. Recursos disponibles en caso de incumplimiento del contrato

Tipos de recursos disponibles

138. Las partes están facultadas para elegir libremente los recursos jurídicos que deseen emplear dentro de los límites previstos por la ley aplicable. Entre ellos cabe mencionar las medidas de reparación en especie que permiten a la parte perjudicada obtener una prestación idéntica o equivalente a la que esperaba recibir si se cumplía el contrato (por ejemplo, la sustitución del equipo físico defectuoso), las compensaciones pecuniarias (por ejemplo, créditos para la utilización de servicios) y la rescisión del contrato. El contrato podría contemplar diferentes tipos de incumplimiento y especificar las medidas que se podrían adoptar en cada caso.

Suspensión o cancelación de los servicios

139. Suspender o cancelar la prestación de los servicios de computación en la nube al cliente es una medida habitual que puede adoptar el proveedor ante un incumplimiento del contrato por parte del cliente, o ante una transgresión de la **PUA** por parte de los usuarios finales del cliente. El contrato puede prever medidas de salvaguardia frente al ejercicio de derechos amplios de suspensión o cancelación. 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 el cliente incurra en un incumplimiento esencial del contrato o en que se presenten amenazas importantes para la seguridad o la integridad del sistema del proveedor, así como a otros supuestos previstos en la ley aplicable. El derecho del proveedor a suspender o cancelar los servicios también puede restringirse únicamente 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, el porcentaje que se descuente puede depender de la medida en que los servicios prestados por el proveedor no se ajusten 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 esos créditos a los casos en que, por ejemplo, los fallos se deban a cuestiones que estén bajo el control del proveedor o disponer que dichos créditos se utilicen dentro de un plazo determinado. Algunos proveedores también pueden estar dispuestos a reembolsar las sumas pagadas u ofrecer un paquete de servicios mejorado durante el período de facturación siguiente (ofreciendo, por ejemplo, consultoría gratuita sobre tecnología de la información). Cuando existen varias opciones disponibles, es posible

que los proveedores establezcan en sus condiciones estándar que serán ellos mismos quienes elegirán la forma de compensar por su incumplimiento.

141. Cuando los créditos para la utilización de servicios son el único recurso previsto contra el incumplimiento por parte del proveedor de sus obligaciones contractuales, el cliente puede ver limitado su derecho a solicitar otras medidas de reparación, como interponer una demanda de daños y perjuicios o resolver el contrato. Además, ofrecer créditos que consistan en un descuento en el precio o un paquete de servicios mejorado en el período de facturación siguiente puede resultar inútil si el contrato se rescinde. Quizás no sea posible exigir el cumplimiento de una cantidad excesiva de créditos si se considera que la estimación de los posibles daños futuros realizada al comienzo del contrato no fue razonable. Otras medidas, como las penalizaciones, pueden ser un incentivo más apropiado para que se cumpla el contrato.

Formalidades que han de seguirse en caso de incumplimiento del contrato

142. En el contrato pueden preverse las formalidades que deben seguirse en los casos de incumplimiento. Por ejemplo, se podría establecer la obligación de la parte que considere que se ha infringido alguna cláusula del contrato de notificar a la otra esa circunstancia, ofreciéndole la oportunidad de subsanar ese incumplimiento. También es posible fijar plazos para solicitar las medidas de reparación.

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 ser diferente de la fecha en que se firma, la fecha en que se acepta la oferta, o la fecha en que se acepta la configuración y se realizan los demás actos necesarios 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 los utilice efectivamente en ese momento. También puede considerarse que la fecha efectiva de entrada en vigor del contrato es la fecha en que el cliente realiza el primer pago por los servicios de computación en la nube, incluso aunque en ese momento el proveedor no los haya puesto todavía a disposición del cliente. 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 un plazo inicial determinado (corto o mediano) con prórrogas automáticas, salvo que el contrato sea rescindido por alguna de las partes. El proveedor puede convenir en notificar al cliente cuando el plazo del contrato esté próximo a vencer. Para tomar una decisión sobre la renovación deben tenerse en cuenta diversas cuestiones, como evitar el riesgo de **dependencia** y el poder conseguir mejores condiciones.

Extinción del contrato

145. Por lo general, en el contrato se establecen las causas que, además del vencimiento del plazo fijado en él, pueden dar lugar a su extinción, como la conveniencia de las partes, el incumplimiento u otros motivos. Es posible que el contrato prevea distintas modalidades de rescisión anticipada, y cuestiones conexas como la obligación de notificar con suficiente antelación, la **reversibilidad** y otras obligaciones relativas a la finalización de los servicios (véanse los párrs. 157 a 167 *infra*).

Rescisión del contrato por razones de conveniencia

146. En sus cláusulas estándar, especialmente las relativas a la prestación de **soluciones de nube genéricas y estandarizadas para múltiples suscriptores**, los proveedores suelen reservarse el derecho a rescindir el contrato en cualquier momento, sin necesidad de que exista incumplimiento del cliente. Las partes pueden convenir en limitar las circunstancias en que se podrá ejercitar este derecho y obligar al proveedor a que notifique al cliente con suficiente antelación su voluntad de rescindir el contrato.

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

Rescisión por incumplimiento

148. Todo incumplimiento esencial del contrato justifica generalmente la rescisión de este. Para evitar ambigüedades, las partes pueden definir en el contrato los supuestos que se considerarán un incumplimiento esencial. El incumplimiento esencial del contrato por parte del proveedor puede consistir en la pérdida o el uso indebido de los datos, la transgresión de la política de protección de datos personales, la recurrencia de los **incidentes de seguridad** (cuando se produzcan, por ejemplo, más de un determinado veces en el 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 parte del cliente y la transgresión de la **PUA** por el cliente o sus usuarios finales son algunos de los motivos más comunes por los que los proveedores rescinden los contratos. El derecho de las partes a rescindir el contrato puede estar sometido a la condición de que se realice una notificación previa, de que se celebren consultas de buena fe, de que se ofrezca la posibilidad de subsanar el incumplimiento y de que no se haya asumido el compromiso de reanudar el cumplimiento del contrato en un determinado número de días a partir de la adopción de las medidas correctivas.

149. En el contrato pueden establecerse las obligaciones del proveedor relacionadas con la finalización de los servicios 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*).

Rescisión 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 rescisión del contrato. Entre ellas podrían citarse las modificaciones de los **requisitos de ubicación de los datos** o las condiciones de subcontratación. El contrato puede conferir al cliente el derecho a rescindir el contrato en su totalidad cuando las modificaciones introducidas en él a causa de una reestructuración de la cartera de servicios del proveedor tuvieran como resultado la cancelación o sustitución de algunos servicios (véanse los párrs. 105 a 124 *supra* y el párr. 155 *infra*).

Rescisión en caso de insolvencia

151. Es posible que se detecte un riesgo de insolvencia cuando se evalúen los riesgos (véase la primera parte, párr. 15 j)) y durante el contrato si, por ejemplo, este exige que se presenten informes periódicos acerca de la situación financiera de las partes. Las cláusulas que permiten rescindir el contrato en caso de insolvencia de una de las partes son bastante frecuentes. No obstante, pueden existir normas imperativas en el régimen legal de la insolvencia que dejen sin efecto esas cláusulas.

152. Es posible que un cliente insolvente 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 rescindir el contrato cuando no concurriera otro, por ejemplo, la falta de pago del cliente.

153. Las partes pueden establecer en el contrato mecanismos que permitan al cliente recuperar sus datos en caso de insolvencia del proveedor (por ejemplo, la liberación automática del código fuente o las claves de custodia para tener acceso a sus datos y otros contenidos), o pueden existir disposiciones legales que prevean esos mecanismos. De lo contrario, el cliente puede tener dificultades para recuperar sus datos y otros contenidos alojados en la infraestructura de nube del proveedor insolvente o tardar en recuperarlos. Cuando se retira una gran cantidad de contenidos como consecuencia de una crisis de confianza ocasionada por la situación financiera del proveedor, tanto el proveedor insolvente como el **representante de la insolvencia** pueden limitar la cantidad de contenido (datos y código de las aplicaciones) que pueden retirarse en un período determinado, o decidir que las obligaciones relativas a la finalización de los servicios se cumplan por orden cronológico.

Rescisión en caso de cambio de control

154. El cambio de control puede suponer, por ejemplo, un cambio en la titularidad o en la capacidad de determinar, directa o indirectamente, las políticas operacionales y financieras del proveedor, lo que puede dar lugar a cambios en la cartera de servicios que este ofrece. El cambio del control también puede entrañar la cesión o la novación del contrato, con la consiguiente transmisión a un tercero de los derechos y las obligaciones (o solo los derechos) previstos en el contrato. Como resultado de ello, es posible que cambie alguna de las partes contratantes originales o que se modifiquen ciertos aspectos del contrato, de modo que, por ejemplo, los pagos deban realizarse a un tercero.

155. La ley aplicable puede disponer que se rescinda el contrato si, como consecuencia del cambio de control, no pudieran cumplirse los requisitos exigidos por las normas legales imperativas (por ejemplo, los **requisitos de ubicación de los datos** o la prohibición de hacer negocios con determinadas entidades porque estuvieran sujetas a un régimen internacional de sanciones o por motivos de seguridad nacional). Los contratos públicos pueden verse especialmente afectados por restricciones legales impuestas a los cambios de control. Además, las partes pueden pactar la posibilidad de rescindir el contrato, en especial si, como consecuencia del cambio de control, 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. Es frecuente que se establezca la obligación de notificar con antelación un próximo cambio de control, así como los efectos que se prevé tenga ese cambio sobre el contrato.

Cláusula sobre cuentas inactivas

156. La inactividad del cliente durante un determinado período de tiempo especificado en el contrato puede dar derecho al proveedor a rescindir unilateralmente dicho contrato. Sin embargo, no es habitual que se incluya la cláusula de cuentas inactivas en los contratos de computación en la nube celebrados entre empresas a título oneroso.

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 el interés del cliente en disponer de acceso continuo a sus datos y otros contenidos (incluso durante el período de transición) y el del proveedor en poner fin lo antes posible a toda obligación que pudiera tener con el cliente anterior.

158. Las obligaciones relativas a la finalización de los servicios pueden ser las mismas, independientemente de la causa de extinción del contrato, o pueden variar según si el contrato se rescinde por incumplimiento o se extingue por otras razones. A continuación se exponen algunas de las cuestiones que quizás convenga a las partes prever en el contrato.

Plazo para la exportación

159. Las partes pueden estipular en el contrato un plazo para la exportación que quizás deba ser suficientemente prolongado para que la transferencia de los datos y otros contenidos del cliente a otro sistema se realice sin tropiezos.

Acceso del cliente al contenido que se ha de exportar

160. El contrato debería especificar 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 puedan 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 dar acceso automático al cliente al código fuente, las claves de descifrado u otros elementos que permitan el acceso a sus datos y otros contenidos cuando se produzcan determinados acontecimientos, como la extinción del contrato (véase también el párr. 153 *supra*)). El contrato también puede especificar, en la medida de lo posible, las diferentes opciones que existen para la exportación, incluidos sus formatos y procesos, aunque aclarando que pueden cambiar con el tiempo.

Asistencia prestada por el proveedor para la exportación

161. Es posible que el proveedor no siempre esté dispuesto a ayudar activamente al cliente a exportar sus datos a otro sistema, pero su deber de garantizar que esa exportación sea posible y fácil de realizar puede estar implícito en la ley. Cuando las partes convienen en que el proveedor participe 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, incluidos el alcance, el procedimiento y la duración de dicha asistencia. El proveedor puede exigir un pago aparte por la prestación de asistencia para la exportación. En ese caso, las partes pueden fijar en el contrato la cuantía de dicho pago o convenir en remitirse al listado de precios del proveedor que esté vigente en un momento dado. Otra posibilidad consistiría en que las partes acordaran que esa asistencia estuviera incluida en el precio del contrato o que no se cobrara ninguna suma adicional si el contrato se rescindiera 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 la exportación o cuando haya vencido el plazo establecido en el contrato para llevar a cabo la exportación. El proveedor puede eliminar los datos automáticamente, por ejemplo, cuando se produzcan determinados acontecimientos, cuando venzan los plazos acordados por las partes o cuando la ley lo exija. Como alternativa a lo anterior, cabría estipular que los datos puedan eliminarse solo cuando el cliente lo solicite 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 en que se le entregue un certificado, informe o declaración sobre los datos eliminados, incluidos los que estuvieran almacenados en sistemas de terceros.

Conservación de los datos una vez extinguido el contrato

163. El proveedor podría estar obligado por ley, en especial por las leyes de protección de datos, a conservar los datos del cliente, por un plazo que también podría estar fijado en la ley. Las partes pueden acordar que se autorice al proveedor a conservar los datos del cliente una vez extinguido el contrato. Algunos proveedores quizás 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 con respecto a los datos que no se devolverán o que no podrán devolverse al cliente y cuya eliminación no será posible. Por ejemplo, el contrato puede establecer la obligación de anonimizar toda información personal y exigir que los datos se conserven cifrados o en un formato utilizable e interoperable que permita recuperarlos en caso necesario. Las partes pueden pactar también sus respectivas obligaciones en relación con la conservación de los datos en el formato especificado una vez extinguido el contrato.

Cláusula de confidencialidad para después de la extinción del contrato

165. Las partes pueden pactar una cláusula de confidencialidad para después de la extinción del contrato. Las obligaciones de confidencialidad pueden subsistir durante un determinado número de años a partir de la extinción del contrato (por ejemplo, durante un plazo de cinco o siete años) o prolongarse indefinidamente, en función de la naturaleza de los datos y otros contenidos del cliente que estuviesen alojados en la infraestructura de nube del proveedor.

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 de distribución de 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 convenir en 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 de resolver sus controversias contractuales. Entre los mecanismos de solución de controversias figuran la negociación, la mediación, la conciliación, la solución de controversias en línea (ODR), el arbitraje y el proceso judicial. Diferentes tipos de controversias pueden justificar que se utilicen distintos procedimientos. Por ejemplo, es posible que los litigios 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 otro tipo de controversias tal vez se resuelvan más eficazmente mediante negociaciones directas entre las partes. En el caso de reclamaciones de poca cuantía, la mediación o la negociación asistida con sistemas ODR pueden ofrecer a las partes métodos rápidos y económicos de alcanzar un acuerdo consensuado en línea. En el caso de reclamaciones de mayor cuantía, los sistemas ODR específicos del sector de nube pueden ofrecer un foro especializado y competente y resultar de utilidad en los procesos judiciales. El derecho vigente en algunas jurisdicciones a veces obliga a las partes a recurrir a determinados mecanismos alternativos de solución de controversias que las partes deben agotar antes de poder someter su controversia a la decisión de un órgano jurisdiccional.

Proceso arbitral

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 pueden ser sometidas a arbitraje; es posible que la ley disponga que

algunas de ellas solo puedan ser decididas por un tribunal judicial. Las partes deberían, por tanto, verificar si las cuestiones en disputa pueden ser sometidas a arbitraje antes de optar por esa vía. Cuando se incluye una cláusula de arbitraje en el contrato, se suele indicar en ella el reglamento de arbitraje por el que se regirá el proceso arbitral. En el contrato puede figurar 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 eligen una institución arbitral, por el reglamento de dicha institución.

Solución de controversias en línea

170. Las partes pueden optar por un mecanismo ODR para resolver algunos tipos de controversias (o todas ellas) derivadas de su contrato, a reserva de las limitaciones impuestas por la ley. El contrato puede especificar el alcance de las cuestiones que podrán someterse a un sistema ODR, la plataforma ODR que se utilizará y las normas que regirán las actuaciones. En algunos casos, el sistema ODR podría venir incluido en el paquete de servicios de nube ofrecido por el proveedor, con la posibilidad de excluirlo en forma voluntaria.

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 y este se comunica con las partes para tratar de que lleguen a un arreglo; y c) una etapa final, en que el administrador ODR o el tercero neutral informan a las partes de la naturaleza de la etapa final y de su forma. El resultado del proceso ODR puede no ser vinculante para las partes, salvo que el contrato o la ley aplicable dispongan lo contrario.

Proceso judicial

172. En caso de iniciarse un proceso judicial podría suceder que, debido a la naturaleza de los **servicios de computación en la nube**, varios Estados considerasen tener competencia para entender en el litigio. En la medida de lo posible, es conveniente que las partes convengan en una cláusula que las obligue a someter sus controversias a un órgano judicial determinado (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 para la participación del cliente en el proceso de solución de controversias (por ejemplo, para fundamentar una demanda o una reconvención). El contrato puede establecer expresamente que, en caso de que surja una controversia entre las partes, el proveedor deberá conservar 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. Asimismo, las partes 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 el cual podrán presentarse reclamaciones. No obstante, si resultaran aplicables los plazos de prescripción establecidos en la ley, las estipulaciones contractuales que no se ajustaran a dichos plazos quedarían sin efecto.

O. Cláusulas de elección de la ley y el foro

175. La libertad contractual (véase el párr. 34 *supra*) normalmente permite que las partes elijan la ley que se aplicará a su contrato y la jurisdicción o el foro en que serán examinadas sus controversias. No obstante, y en función del objeto de la controversia,

es posible que existan normas legales imperativas (por ejemplo, la legislación sobre protección de datos) que prevalezcan sobre las cláusulas de elección de la ley y el foro pactadas por las partes contratantes. Además, independientemente de la ley y el foro que las partes elijan, es posible que resulte aplicable al contrato más de un conjunto de normas legales imperativas (por ejemplo, la legislación sobre protección de datos, el régimen legal de la insolvencia, etc.), incluso de diferentes jurisdicciones.

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

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

177. Al elegir el foro, las partes suelen tener en cuenta los efectos de la ley elegida o de la que resultara aplicable y en qué medida se reconocerá y aplicará una resolución judicial de ese foro en los países en los que probablemente se solicite su ejecución. Quizás sea importante mantener la flexibilidad en cuanto a los métodos de ejecución posibles, especialmente en los entornos de computación en la nube en que puede resultar difícil determinar ciertos factores que las partes suelen tener en cuenta al redactar las cláusulas de elección de la ley y el foro, como la ubicación de los bienes utilizados para la prestación de los servicios y la ubicación del proveedor y del cliente.

Ley y foro obligatorios

178. Una controversia puede tener que someterse obligatoriamente a la ley y el foro de una jurisdicción determinada por diversos motivos, entre ellos los siguientes:

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

b) que la nacionalidad o el domicilio del **sujeto de los datos** o de las partes contratantes, en especial del **responsable de los datos**, den lugar a la aplicación de la ley del **sujeto de los datos** o la parte afectados; y

c) que la ley del lugar en que se originó la actividad (la ubicación del equipo) o del lugar al que se dirige la actividad con fines de lucro dé lugar a la aplicación de la ley de ese lugar. La utilización de un dominio de nivel superior de un determinado país vinculado a un lugar determinado, un sitio web en el idioma local, precios fijados en la moneda local y personas de contacto locales son algunos de los factores que podrían influir en esa determinación.

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 rigen por la ley de la sede principal de los negocios, o establecimiento principal, del proveedor. En ellos se otorga normalmente a los órganos jurisdiccionales del país del proveedor competencia exclusiva sobre todas las controversias derivadas del contrato. El cliente tal vez prefiera la ley y el foro de su propio país. Por lo general, pesan sobre las entidades públicas importantes restricciones para aceptar la ley de otro país y la competencia de tribunales extranjeros. Es posible que los proveedores que realizan sus actividades en varias jurisdicciones sean flexibles 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 pueden prever asimismo diversas opciones en cuanto a la ley y el foro que serán aplicables a los diferentes aspectos del contrato. También pueden optar por la jurisdicción del demandado, para que el demandante no cuente con 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 ley y foro

181. Las partes pueden preferir no incluir cláusulas de elección de la ley y el foro en su contrato, dejando la cuestión abierta para ser tratada más adelante, de ser necesario. En algunos casos, esta solución podría considerarse la única 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. Las cláusulas relativas a las notificaciones 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 (el momento de la entrega, del envío o del acuse de recibo). A falta de disposiciones legales imperativas, las partes pueden acordar las formalidades que habrán de utilizar para efectuarlas, que pueden ser uniformes o variar según el grado de importancia de la notificación, su urgencia y otras consideraciones. Por ejemplo, es posible que se exijan formalidades más estrictas para las notificaciones de suspensión o rescisión unilateral del contrato que para las notificaciones ordinarias. Las partes pueden pactar los plazos de notificación, teniendo presente que debe permitirse la **reversibilidad** y la continuidad de las operaciones. El contrato puede hacer referencia a las notificaciones y los plazos impuestos por la ley.

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

Q. Otras cláusulas

184. A menudo las partes agrupan bajo el título “otras cláusulas” diversas cláusulas para las que no encuentran una ubicación más adecuada en otras partes del contrato. Algunas de ellas (denominadas “cláusulas tipo”) tienen una redacción estándar que suele usarse en todo tipo de contratos mercantiles, como la cláusula de divisibilidad, que permite 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 demás versiones 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 modificaciones al contrato. En este debería establecerse el procedimiento que ha de seguirse para introducir modificaciones y para que estas surtan efectos. También puede ser necesario prever en el contrato las consecuencias que tendría el rechazo de las modificaciones por cualquiera de las partes.

186. Habida cuenta de la naturaleza de los **servicios de computación en la nube**, podría ser difícil distinguir entre los cambios que supondrían una modificación 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 constituiría necesariamente una modificación del contrato inicial, como tampoco constituirían una modificación 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 y de cambiar el precio como consecuencia de esa adición puede constituir una modificación del contrato. Las actualizaciones que produzcan cambios sustanciales en las condiciones y políticas acordadas previamente también pueden constituir una modificación del contrato.

187. El grado en que se permite modificar 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 convenidas originalmente, convendría que cada una de las partes guardara separadamente la totalidad de las cláusulas acordadas inicialmente y sus modificaciones.

Glosario

Acuerdo sobre la cantidad y calidad de los servicios (SLA): parte del contrato de computación en la nube celebrado entre el proveedor y el cliente en 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 rendimiento).

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 y su uso, y para garantizar la integridad de los datos. La auditoría puede ser interna o externa, o realizada por un tercero independiente nombrado por el proveedor, el cliente o ambas partes. En el **acuerdo sobre la cantidad y calidad de los 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 apoyan las actividades del proveedor, del cliente o de ambos o que colaboran en esas actividades. Los auditores de nube realizan la **auditoría** de la prestación y el uso de los **servicios de computación en la nube**. Los intermediarios de servicios de nube o los integradores de sistemas ayudan a las partes en relación con una amplia gama de cuestiones, por ejemplo, encontrar la solución de nube más adecuada, negociar condiciones aceptables y migrar los contenidos del cliente a la nube.

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

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 los datos personales en algunas jurisdicciones puede abarcar cualquier dato o información directa o indirectamente vinculada o relacionada con una persona identificada o identificable (véase la definición de **sujeto de los datos**).

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

Derechos de los sujetos de los datos: derechos relacionados con 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 relacionados con sus datos personales, como la ubicación de esos datos, su utilización por terceros, la filtración de datos u otras infracciones relacionadas con 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 el **procesamiento** de sus datos personales y a que se le garantice la **portabilidad** de sus datos personales.

Eliminación de datos: secuencia de operaciones diseñadas para borrar datos en 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 los datos. En el **acuerdo sobre la cantidad y calidad de los servicios (SLA)** pueden establecerse un parámetro cuantitativo y 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 determinado 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 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 su utilización por el ser humano como a su procesamiento informático.

Incidente de seguridad: acontecimiento que indica que el sistema o los datos han corrido peligro o que han fallado las medidas adoptadas para protegerlos. Un incidente de seguridad perturba el funcionamiento normal del sistema. Como ejemplos de incidentes de seguridad pueden citarse los intentos de acceso no autorizados al sistema o los datos, la interrupción imprevista de un servicio o la denegación de un servicio, el procesamiento o almacenamiento no autorizado 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 físicos ni virtuales, pero tiene el control de los sistemas operativos, el almacenamiento y las aplicaciones instaladas que utilicen los recursos físicos y virtuales. El cliente puede tener también una posibilidad limitada de controlar determinados componentes de red (por ejemplo, los cortafuegos locales).

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

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 sobre la cantidad y calidad de los servicios (SLA)**, la latencia suele estar expresada en milisegundos.

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

Metadatos: información básica sobre los datos (como su autor, su fecha y hora de creación, su fecha y hora 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: las 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:

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

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

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

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

Normativa propia de cada sector: normas aplicables a los sectores financiero, sanitario o público u otros sectores o profesiones (por ejemplo, las 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 información de acceso restringido por ley o reglamento a 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 se especifica en el contrato un RPO de las dos horas anteriores a la interrupción de los servicios, ello significa que tras la recuperación se podrá acceder a todos los datos en la forma que tenían dos horas antes de producirse la interrupción.

Objetivos de tiempo de recuperación (RTO): 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 implantado una política de administración de claves en cumplimiento de las normas internacionales señaladas 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 de las necesidades del negocio (por ejemplo, la importancia crítica de determinados datos, servicios o aplicaciones y las correspondientes prioridades de recuperación). Por ejemplo, un sistema no esencial diseñado para utilizar la nube con fines de archivo no necesitaría el mismo **período de disponibilidad** u otras condiciones previstas en el **acuerdo sobre la cantidad y calidad de los 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 sobre la cantidad y calidad de los 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 la 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 la 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 o programas informáticos creados o adquiridos por él utilizando alguno o algunos 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 que define 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 precio, con el menor trastorno posible y sin necesidad de volver a introducir los datos, reorganizar los procesos o reprogramar las aplicaciones). Esto podría lograrse si fuera posible recuperar los datos en un formato que fuese aceptado por otro sistema o mediante una transformación simple y directa utilizando instrumentos normalmente disponibles. En el **acuerdo sobre la cantidad y calidad de los 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 para programas de aplicación documentados; o que el formato de los datos esté suficientemente estructurado y documentado para permitir que el cliente lo reutilice o lo reestructure, si se quiere, en un formato diferente.

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

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

Reversibilidad: proceso que debe seguirse para que el cliente recupere de la nube sus datos, aplicaciones y otros contenidos conexos y para que el proveedor elimine los datos y otros contenidos conexos del cliente después del 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, con arreglo a las necesidades del cliente, teniendo en cuenta las grandes tendencias en el uso 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 tengan control o conocimiento de los procesos involucrados;

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 el uso de la gama completa de la infraestructura física de tecnología de la información (como servidores y centros de datos) y los recursos virtuales necesarios para que el cliente construya sus propias plataformas de tecnología de la información, o despliegue, administre y ejecute las aplicaciones o los programas informáticos adquiridos o creados 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: cuando el proveedor no es propietario de la totalidad o una parte 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 todos o algunos de los **servicios de computación en la nube**. Por ejemplo, el proveedor de servicios **PaaS** o **SaaS** puede utilizar la infraestructura de almacenamiento y servidores (centros de datos, servidores de datos) que sean propiedad de otra entidad o sean proporcionados por esta. Como resultado de ello, podrían participar en la prestación al cliente de los servicios de computación en la nube uno o más subproveedores. El cliente quizás no sepa qué niveles participan en la prestación de los servicios en un momento dado, lo que hace difícil determinar y gestionar los riesgos. Los servicios estratificados de computación en la nube son comunes, especialmente en la modalidad **SaaS**.

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

Sujeto de los datos: persona física que puede ser identificada, directa o indirectamente, a través de los datos, por ejemplo, por referencia a datos de identificación 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, los sujetos de los datos gozan, conforme a las normas sobre protección o privacidad de los datos, de determinados derechos sobre los datos que permitan identificarlos. Esas normas pueden dar lugar a la inclusión en el **acuerdo sobre la cantidad y calidad de los servicios (SLA)** de parámetros cuantitativos y cualitativos específicos sobre protección de datos, por ejemplo, que un auditor independiente certifique, al menos una vez al año, que los servicios prestados en virtud del contrato cumplen la norma de 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.