

# InterPARES Trust



## *Lista de verificación para contratos de servicios en la nube Versión final*

Este trabajo está disponible mediante la  
**Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Public License**  
<http://creativecommons.org/licenses/by-nc-sa/4.0/>



Title:Título:	Lista de verificación para los contratos de servicio en la nube
Status:	<b>FINAL</b>
Version:	2.0
Fecha de entrega:	October 2015 Octubre 2015
Última revision:	February 26, 2016 Febrero 26, 2016
Autor:	InterPARES Trust Project Proyecto InterPARES Trust
Escritores:	Jessica Bushey, Marie Demoulin, Elissa How and Robert McLelland
Dominio de investigación	Team Norteamérica-Legal-NA14
Traducción al español fecha	Agosto, 2016
Traductora	Alicia Barnard
Revisión:	Juan Voutssás, Fiona Aranguren Celorrio, Lluís-Esteve Casellas i. Serra.

La siguiente lista de verificación para los contratos de servicios en la nube es un producto final de investigación que llevó a cabo el Proyecto InterPARES Trust sobre contratos comunes de servicio desde una perspectiva de administración de archivos, archivística y jurídica. InterPARES Trust (2013-2018) es un proyecto de investigación multinacional, interdisciplinario que explora cuestiones relacionadas con los documentos de archivo y datos en el ambiente en línea. Para mayor información ver <https://interpares.org>.

Las audiencias objetivo para este documento son los gestores o administradores de documentos, archivistas, funcionarios de servicios de información y otros interesados que evalúan los servicios de nube dentro de una organización. El objetivo del mismo es proporcionar una herramienta para:

- Adquirir un conocimiento de un texto estándar o modelo de contratos.
- Verificar si los contratos potenciales de servicios en la nube cumplen con los requerimientos.
- Clarificar a las áreas de tecnologías de la información y jurídicas las necesidades de gestión documental y archivísticas
- Comunicar las necesidades de gestión documental y archivística a los proveedores de servicio de nube.

Esta lista de verificación es solo una herramienta para tomar en cuenta, no constituye una propuesta jurídica. No se recomienda su uso para o en contra de cualquier proveedor de servicio de nube en particular (o uso de servicios de nube en general). Los individuos y las organizaciones deberán solicitar el apoyo jurídico en caso de que lo requieran para un contrato en particular.

## Lista de verificación para contratos de servicios en la nube Público objetivo: Gestores documentales y archivistas<sup>1</sup>

Preguntas	sí	no	? <sup>2</sup>	Notas
<b>1. Convenio</b>				
▪ ¿Se encuentra claramente establecida la fecha efectiva de inicio del contrato?				
▪ ¿Existe una explicación sobre las circunstancias por las cuales el servicio podría suspenderse?				
▪ ¿Existe una explicación sobre las circunstancias por las cuales el servicio podría darse por concluido? (ver también sección 8)				
▪ ¿Existe una explicación de notificación o una opción para suscribir un servicio de notificación en el caso de cambios realizados a los términos que regulan el servicio? <sup>3</sup>				
<b>2. Propiedad de la información y uso</b>				
▪ ¿Se retiene la propiedad de los datos que almacena, transmite, y/o produce en el servicio de nube?				
▪ ¿Se reserva el proveedor el derecho para usar los datos para propósitos de operar y mejorar los servicios?				
▪ ¿Se reserva el proveedor el derecho para usar los datos con propósitos de mercadotecnia?				

<sup>1</sup> La lista de verificación es principalmente una herramienta para apoyar a las organizaciones a evaluar cuestiones típicas de un formato estándar para convenios de cómputo en la nube, en los cuales la organización tiene que negociar con convenios propuestos por el proveedor. Una segunda aplicación de la lista es proporcionar un panorama de cuestiones sobre gestión documental que son relevantes para los servicios de cómputo en la nube y que deberían estar incluidos en los términos del convenio. Se hace énfasis que cualquier organización en proceso de adquisición de servicios de cómputo en la nube, donde se el contrato del cliente se está elaborando, deberá revisarse cuidadosamente y contar con el consejo jurídico necesario sobre los términos de uso específicos.

<sup>2</sup> La columna “?” indica una situación en la cual el contrato no es claro o la cuando pregunta no aplica al contrato en particular.

<sup>3</sup> Algunos convenios de servicios de nube, especialmente servicios en la nube pública, incluyen cláusulas que permiten al proveedor cambiar los términos del convenio en cualquier momento y a su discreción. Por tanto, si es posible las organizaciones deberían considerar eliminar este derecho o hacer que el mismo esté sujeto al acuerdo de la organización para hacer cualquier cambio, o asegurar que el proveedor esté obligado a notificar a la organización con bastante anticipación de cualquier cambio.

<ul style="list-style-type: none"> <li>¿Se reserva el proveedor el derecho para usar o disponer de sus datos como datos abiertos anónimos (a través de aplicaciones API's)?</li> </ul>				
<ul style="list-style-type: none"> <li>¿El proveedor restringe el tipo de contenido que usted almacena en cumplimiento a legislación sobre derechos de autor y otros derechos de propiedad intelectual?</li> </ul>				
<ul style="list-style-type: none"> <li>Los términos del proveedor ¿Aplican a metadatos?<sup>4</sup></li> </ul>				
<ul style="list-style-type: none"> <li>¿Se adquiere la propiedad de los metadatos generados por el sistema de servicio de nube, durante los procedimientos para subir, administrar, recuperar y migrar datos?</li> </ul>				
<ul style="list-style-type: none"> <li>¿Se tienen derechos para acceder a estos metadatos durante la relación contractual (ver también la sección 8)</li> </ul>				
<b>3. Disponibilidad, recuperación y uso</b>				
<ul style="list-style-type: none"> <li>¿Son precisos los indicadores proporcionados respecto de la disponibilidad del servicio?</li> </ul>				
<ul style="list-style-type: none"> <li>¿Se cumplen las necesidades de la organización en cuanto al grado de disponibilidad de datos?</li> </ul>				
<ul style="list-style-type: none"> <li>¿Permite el grado de disponibilidad de datos cumplir con las leyes de acceso a la información?<sup>5</sup></li> </ul>				
<ul style="list-style-type: none"> <li>¿Permite el grado de disponibilidad de los datos cumplir con el derecho de las personas para acceder a sus datos personales?<sup>6</sup></li> </ul>				
<ul style="list-style-type: none"> <li>¿Permite el grado de disponibilidad de los datos cumplir con el derecho de las autoridades para acceder legalmente a la investigación de sus datos para fines de investigación, control o propósitos judiciales?</li> </ul>				
<ul style="list-style-type: none"> <li>¿Se encuentran claramente establecidos los procedimientos, el tiempo y el costo para restaurar los datos después de una interrupción del servicio?</li> </ul>				

<sup>4</sup> Los metadatos aseguran que los documentos de archivo puedan ser hallados, recuperados y utilizados. Son críticos para asegurar la autenticidad de los mismos al paso del tiempo. Pueden ser generados por la organización o por el proveedor. Es por lo tanto importante abordar específicamente los metadatos en el contrato a fin de clarificar cuestiones tales como propiedad, acceso, retención y disposición durante el servicio y después de su terminación.

<sup>5</sup> En general, las leyes de acceso a la información permiten el acceso por cualquier persona a la información guardada por los gobiernos en los países.

<sup>6</sup> En algunos países existe una ley de privacidad que protege la privacidad de los individuos con respecto a su información personal acerca de ellos mismos guardada por organismos públicos y/o privados y que les da derecho a acceder a esa información.

4. Almacenamiento de datos y preservación				
4.1. Almacenamiento de datos				
▪ ¿El proveedor genera copia de seguridad <sup>7</sup> de los datos de la organización?				
▪ En el caso de que la organización maneje documentos de archivo externos (ejem. Datos del cliente), ¿El proveedor genera copia de seguridad de sus clientes?				
▪ Los términos del proveedor ¿Aplican a cualquier copia de seguridad generado? <sup>8</sup>				
▪ En el caso de supresión accidental de datos, ¿tiene el proveedor la responsabilidad de la recuperación de datos?				
4.2. Preservación de datos				
▪ ¿Existen procedimientos definidos para indicar que sus datos serán manejados al paso del tiempo de manera que preserven su usabilidad, fiabilidad, autenticidad e integridad? <sup>9</sup>				
▪ ¿Existen procedimientos para asegurar la integridad del archivo durante la transferencia de los datos dentro y fuera del sistema? (ejem. “checksums”)				
▪ ¿Se proporciona alguna explicación acerca de cómo evolucionará el servicio en el tiempo (es decir actividades de migración y/o emulación)?				
▪ ¿Proporciona el sistema acceso a bitácoras de auditoría <sup>10</sup> respecto de las actividades relacionadas con la evolución del servicio?				
▪ ¿Habrá una notificación del proveedor sobre los cambios realizados a sus datos debido a la evolución del servicio?				
▪ ¿Puede solicitarse una notificación de cambios inminentes al sistema respecto de la evolución del servicio que puedan impactar a sus datos?				

<sup>7</sup> Nota de traducción. En español el término “backup” también se traduce como: “respaldo de datos”, “respaldo de información” o “copia de información”.

<sup>8</sup> Específicamente en términos de propiedad, acceso, seguridad, retención y disposición durante el servicio y después de su conclusión.

<sup>9</sup> La usabilidad, fiabilidad, autenticidad e integridad se pueden definir en el contrato (por ejem. En una sección de definiciones o en el glosario). Se recomienda verificar si la organización y el proveedor tienen un entendimiento común de estos conceptos.

<sup>10</sup> Nota de traducción. En español el término “audit trail” también se traduce como “pista de auditoría”.

<b>5. Retención y Disposición de datos</b>				
▪ ¿Está informado acerca del procedimiento y condiciones para la destrucción de sus datos? <sup>11</sup>				
▪ ¿Sus datos (y todas las copias, incluyendo respaldos) serán destruidos en cumplimiento con las disposiciones establecidas (disposición documental)?				
▪ Si es así, ¿Serán destruidos inmediata y permanentemente de tal manera que su reconstrucción no sea posible, de acuerdo con la política o lineamiento para una destrucción segura que asegure la confidencialidad de los datos hasta su eliminación completa?				
▪ ¿Existe información disponible acerca de la naturaleza y contenido de los metadatos asociados que son generados por el sistema de servicio de nube?				
▪ ¿El proveedor destruirá los metadatos asociados al momento de disposición final de sus datos?				
▪ ¿El proveedor enviará y/o proporcionará acceso a las bitácoras de auditoría de la actividad de destrucción?				
▪ ¿El proveedor proporcionará una certificación, reporte o declaración de eliminación (si es requerido por las políticas legales de destrucción)?				
<b>6. Seguridad, confidencialidad y privacidad</b>				
<i>6.1 Seguridad</i>				
▪ ¿Impide el sistema acceso, uso, alteración o destrucción de sus datos?				
▪ ¿Están seguros los datos durante los procedimientos de transferencia dentro y fuera del sistema?				
▪ ¿Proporciona y da acceso el sistema a las bitácoras de auditoría, metadatos, y/o bitácoras de acceso <sup>12</sup> para demostrar las medidas de seguridad?				
▪ ¿Se notificará en el caso de una violación a la seguridad o un mal funcionamiento del Sistema?				

<sup>11</sup> Por ejemplo, ¿La operación es automática o requiere autorización de la organización? ¿Ofrece el proveedor la función de “congelamiento” para suspender temporalmente la disposición de un grupo de datos y/o metadatos en contraposición de las instrucciones de la tabla de vigencias? For example, is this operation automatic or does it require your authorization? ¿Se hará saber a la organización o podrá especificar el método de disposición?

<sup>12</sup> Nota de traducción. En español el término “bitácoras de acceso” también se utiliza como anglicismo parcial “logs de acceso”.

<ul style="list-style-type: none"> <li>▪ ¿Usa el proveedor servicios de un subcontratista?</li> </ul>				
<ul style="list-style-type: none"> <li>▪ ¿Ofrece información el proveedor acerca de la identidad del subcontratista y sus tareas?</li> </ul>				
<ul style="list-style-type: none"> <li>▪ ¿Se encuentran los subcontratistas en el mismo nivel de obligaciones legales de las del proveedor del servicio de nube?</li> </ul>				
<ul style="list-style-type: none"> <li>▪ ¿Existe un plan de recuperación de desastres disponibles, o el contrato considera qué pasa en el evento de un desastre?</li> </ul>				
<ul style="list-style-type: none"> <li>▪ ¿Ofrece el proveedor cualquier información relacionada con resultados anteriores respecto de los procedimientos de recuperación de desastres?</li> </ul>				
<b>6.2 Confidencialidad</b>				
<ul style="list-style-type: none"> <li>▪ ¿Cuenta el proveedor con una política de confidencialidad respecto de sus empleados, socios y subcontratistas?</li> </ul>				
<b>6.3 Privacidad</b>				
<ul style="list-style-type: none"> <li>▪ ¿Los términos del proveedor incluyen políticas de privacidad, confidencialidad o seguridad para datos sensibles, confidenciales, personales o de otro tipo especial?</li> </ul>				
<ul style="list-style-type: none"> <li>▪ ¿Está claramente establecido cuál información (incluyendo información personal) es coleccionada acerca de la organización, por qué es coleccionada y cómo será usada por el proveedor?</li> </ul>				
<ul style="list-style-type: none"> <li>▪ ¿Comparte el proveedor esta información con otras compañías, organizaciones o individuos sin su consentimiento?</li> </ul>				
<ul style="list-style-type: none"> <li>▪ ¿Establece razones legales el proveedor por las cuales ellos compartirían la información con otras compañías, organizaciones o individuos?<sup>13</sup></li> </ul>				
<ul style="list-style-type: none"> <li>▪ Si el proveedor comparte esta información con sus afiliados por razones de procesamiento, ¿esto se lleva a cabo en cumplimiento con la política de privacidad, confidencialidad o seguridad existente?</li> </ul>				
<b>6.4. Certificación y auditoría</b>				

<sup>13</sup> Por ejemplo, ¿se sabe que su información puede estar accesible por cumplimiento legal y por autoridades de seguridad nacional de jurisdicciones diferentes?



<ul style="list-style-type: none"> <li>▪ ¿Está el proveedor acreditado en un programa de certificación de terceros?</li> </ul>				
<ul style="list-style-type: none"> <li>▪ El proveedor ¿Es auditado de forma sistemática, regular e independiente por un tercero para demostrar el cumplimiento con políticas de seguridad, confiabilidad y privacidad?</li> </ul>				
<ul style="list-style-type: none"> <li>▪ ¿Está documentada la certificación o proceso de auditoría?</li> </ul>				
<ul style="list-style-type: none"> <li>▪ ¿Se tiene acceso a la información de los organismos de auditoría o certificadores y la fecha de vencimiento de la certificación?</li> </ul>				
<b>7. Ubicación de los datos y flujo de datos transfronterizos</b>				
<i>7.1 Ubicación de los datos</i>				
<ul style="list-style-type: none"> <li>▪ ¿Se sabe dónde se localizan los datos y sus copias durante su almacenamiento en el servicio de nube?</li> </ul>				
<ul style="list-style-type: none"> <li>▪ ¿Se cumple con los requisitos del lugar que pueden ser impuestos a los datos de la organización por ley, especialmente aplicables por la ley de privacidad?</li> </ul>				
<ul style="list-style-type: none"> <li>▪ ¿Se tiene la opción de especificar la ubicación, en la cual sus datos y sus copias serán almacenados?</li> </ul>				
<ul style="list-style-type: none"> <li>▪ ¿Se sabe dónde se almacenan los metadatos y si éstos están almacenados en la misma ubicación de los datos?</li> </ul>				
<i>7.2 Flujo transfronterizo de datos</i>				
<ul style="list-style-type: none"> <li>▪ ¿Se notificará si la ubicación de los datos se mueve fuera de la jurisdicción del cliente?</li> </ul>				
<ul style="list-style-type: none"> <li>▪ ¿Se tienen cuestiones o problemas acerca de los datos almacenados que están sujetos a órdenes de apertura emitidas por autoridades de seguridad nacionales o extranjeras?</li> </ul>				
<ul style="list-style-type: none"> <li>▪ ¿Establece el proveedor claramente la jurisdicción legal en la cual el convenio será cumplido y las disputas potenciales serán resueltas?</li> </ul>				
<b>8. Fin del servicio – Terminación del contrato<sup>14</sup></b>				

<sup>14</sup> El final del servicio es un momento clave que necesita ser abordado en el contrato a fin de especificar el procedimiento a seguir, las obligaciones y responsabilidades de la organización y del proveedor y el destino de todos los datos antes de terminar la relación contractual.

<ul style="list-style-type: none"> <li>▪ En el caso de que el proveedor termine el servicio, ¿Existirá una notificación?</li> </ul>				
<ul style="list-style-type: none"> <li>▪ ¿Existe un procedimiento establecido para contactar al proveedor si se desea terminar el contrato?</li> </ul>				
<ul style="list-style-type: none"> <li>▪ Si el contrato es terminado, ¿Se transferirán los datos a la organización o a otro proveedor de su elección en un formato utilizable e interoperable?</li> </ul>				
<ul style="list-style-type: none"> <li>▪ ¿Está claramente establecido el procedimiento, costo y periodo para devolver/transferir los datos al final del contrato?</li> </ul>				
<ul style="list-style-type: none"> <li>▪ Al final del contrato, ¿Se tiene el derecho para acceder a los metadatos generados por el sistema del servicio de nube?</li> </ul>				
<ul style="list-style-type: none"> <li>▪ Al final del contrato y después de completar el reconocimiento de restitución de los datos ¿Serán los datos y los metadatos asociados inmediata y permanentemente destruidos de tal forma que se impida su reconstrucción?</li> </ul>				
<ul style="list-style-type: none"> <li>▪ ¿Se tiene una opción para confirmar la eliminación de documentos de archive y metadatos por la organización antes de la terminación de los servicios con el proveedor?</li> </ul>				
<ul style="list-style-type: none"> <li>▪ ¿Se cuenta con la opción para el cliente para terminar el acuerdo de servicio sin penalidad en el caso de que el proveedor del servicio de nube cambie?</li> </ul>				