InterPARES Trust

Nombre del estudio :		Asegurar la confianza en el almacenamiento de un servicio de infraestructura en la nube (IAAS por sus siglas en inglés
Nombre del Team y Número del caso de estudio:		EU08
Dominio de investigación:		Infraestructura
Título del documento		Lista de verificación
Status:		Final
Versión:		v1.2
Fecha de envío:		2016/07/27
Última revisión:		2016/08/03
Autor:		InterPARES Trust
Escritores:		Hrvoje Stancic, Faculty of Humanities and Social Sciences, University of Zagreb Edvin Bursic, Financial Agency (FINA) and GRA, Faculty of Humanities and Social Sciences, University of Zagreb Adam Al-Hariri, GRA, Faculty of Humanities and Social Sciences, University of Zagreb
Editor:		Corinne Rogers
Traducción al español		Alicia Barnard
Revisión de traducción		Lluis-Esteve Casellas i. Serra, Fiona Aranguren Celorrio y Juan Voutssás,

Control del documento

Historia de la versión			
Versión	Fecha	Por	Notas de la versión
v 1.1	2016/07/27	Corinne Rogers	Adaptado del reporte final EU08
v 1.2	2016/08/03	Hrvoje Stancic	Mejoras y ediciones menores
v.1.3E			

Lista de verificación en IaaS

Esta lista de verificación está diseñada para brindar orientación a personas, organizaciones, agencias o dependencias de gobierno a fin de evaluar la seguridad y confiabilidad continuada (es decir autenticidad, fiabilidad y precisión) de sus datos cuando se almacenan en una plataforma de infraestructura como servicio (IaaS por sus siglas en inglés). Es el resultado del estudio Garantizar la Confianza en el Almacenamiento en un Servicio como Infraestructura (EU08) en el marco del Proyecto Internacional de Investigación InterPARES Trust (https://interparestrust.org). El objetivo del estudio fue el de establecer una cantidad mínima de información necesaria para sustentar la confianza de los usuarios en un proveedor de IaaS y también posicionar al proveedor como proveedor del servicio de confianza.

En la base de datos terminológica de InterPARES Trust, el término "confianza" se define como "Confianza de una parte en otra, basada en el alineamiento de sistemas de valores con respecto a acciones específicas o beneficios, e involucrando una relación de vulnerabilidad voluntaria, dependencia y confiabilidad, basada en una evaluación de riesgo"[1] Esto significa que los usuarios de servicios de la nube deberían contar con la información suficiente sobre un servicio en particular (ejem. en términos o condiciones del servicio) a fin de confiar en el mismo, o en el acuerdo de nivel de servicios (ANS) entre los usuarios y el proveedor de servicios de nube (PSN) deberían proteger igualmente los intereses de ambas partes involucradas.

Para la mayor comprensión de lo que implican las cuestiones de confianza en servicios de nube, el equipo de investigación elaboró un cuestionario. La lista de verificación está basada en ese cuestionario, el cual fue utilizado durante la recolección de datos para el análisis de proveedores croatas de servicios de nube que ofrecían IaaS. La lista de verificación consiste en 36 preguntas divididas en 10 categorías:

1. Información general (4 preguntas)
2. Gobernanza (4 preguntas)
3. Cumplimiento/conformidad (4 preguntas)
4. Confianza (5 preguntas)
5. Arquitectura (6 preguntas)
6. Identidad y Administración de Acceso (1 pregunta)
7. Aislamiento de datos (2 preguntas),
8. Protección de datos (5 preguntas)
9. Disponibilidad (2 preguntas)
10. Respuesta a incidentes (3 preguntas)

Esta lista puede ser usada por gestores documentales y archivistas cuando evalúan un PSN que ofrece un IaaS así como por PSN como directriz para proveer información en línea acerca del servicio. El informe completo de este estudio puede localizarse en https://interparestrust.org/assets/public/dissemination/EU08_20160727_EnsuringTrustStorageIaaS_FinalReport_Final.pdf.

Lista de Verificación IaaS

	Pregunta	S*	N	?**	Respuesta / Información adicional***
1. Información General					
1.	¿Qué componentes son utilizados en IaaS?				
2.	¿Cuáles son los tipos de servicios ofrecidos en IaaS?				
3.	¿Qué tecnologías se están utilizando?				
4.	¿Qué implicaciones tienen las tecnologías utilizadas en la seguridad y privacidad del sistema?				
2. Gobernanza					
5.	¿Es posible para el cliente monitorizar la seguridad del entorno informático y la seguridad de datos? ¿Cómo?				
6.	¿Qué tipo de seguridad asegura al cliente que sus datos no se mezclan con otros?				
7.	¿Qué tipo de seguridad asegura al cliente que no se comparten datos con empleados de diferente rango y/o que no son creados por otros?				
8.	¿Qué mecanismos de auditoria y herramientas son utilizadas para determinar cómo se almacenan, protegen y utilizan los datos para validar servicios y para verificar la aplicación de la política?				
3. Cumplimiento					
9.	¿Cumple el servicio con legislación, regulaciones, normas y especificaciones para clientes ubicados fuera del país del servicio?				
10.	¿Cómo se protege el servicio contra el acceso no autorizado, el uso, la divulgación, la alteración, la modificación o la destrucción de los datos?				

* Para las respuestas que no tienen opciones simples Si/No/? en los campos sombreados, tiene la opción "?" cuando se requiere una respuesta más elaborada.

** La columna con signo de interrogación "?" indica la situación donde no hay respuesta disponible o que la pregunta no es aplicable en el entorno donde se aplica la lista

*** La columna respuesta/información adicional puede ser usada en casos donde la pregunta no es de tipo Si/No o cuando la respuesta Si/No puede ser complementada con información útil.

11.	¿Qué salvaguardas técnicas y físicas asegura/garantiza el servicio?				
12.	¿El servicio hace uso de subcontratistas para cualquier parte de la tecnología utilizada o del servicio ofrecido?				
4. Confianza					
13.	¿Está el servicio asegurado contra un ataque de rechazo del servicio?				
14.	¿El servicio garantiza la propiedad sobre los datos?				
15.	¿Cuenta el servicio con algún certificado relevante para el mismo?				
16.	¿Qué tipo de gestión del riesgo proporciona la organización?				
17.	¿Qué tipo de seguridad física y lógica está asegurada en los servidores virtuales y en las aplicaciones?				
5. Arquitectura					
18.	¿Cómo está asegurado un hipervisor o monitor de máquina virtual?				
19.	¿Cómo asegura el servicio imágenes de máquina virtual de ataques que buscan el código propietario y los datos?				
20.	¿Utiliza el servicio procesos de gestión para regular la producción, almacenamiento y uso de imágenes de máquina virtual o contenedores?				
21.	¿Cómo se asegura el servicio contra ataques de parte del cliente?				
22.	¿Cómo se asegura el servicio contra ataques del lado del servidor?				
23.	¿Hace el servicio uso de red de intercambio encriptada?				
6. Administración (gestión) de identidad y acceso					
24.	¿Cómo se protege el servicio de datos auxiliares? - datos acerca de cuentas de consumidores, - datos acerca de la actividad relacionada. con el cliente - datos coleccionados para medir y cobrar por el consumo de recursos, - logs, pistas de auditoria y otros, tales como metadatos que son generados y acumulados dentro del entorno,				

	– datos de una iniciativa de la organización (es decir, el nivel de actividad o crecimiento proyectado de una empresa emergente), – metadatos recolectados por el proveedor				
7. Aislamiento de software					
25.	¿Cómo previene el servicio ataques de intermediarios?				
26.	¿Está el servicio asegurado contra ataques al servidor dirigido a contraseñas?				
8. Protección de datos					
27.	¿Qué tipo de encriptación utiliza el servicio para asegurar los datos almacenados en IaaS?				
28.	¿Ha realizado el servicio ataques deliberados a fin de probar la protección del Sistema?				
29.	¿Qué procedimiento se utiliza para la limpieza del servicio a la terminación del mismo, es decir, cómo se asegura el servicio que los datos después de ser suprimidos no son recuperables?				
30.	¿Dónde se almacenan los datos geográficamente?				
31.	¿Dónde se almacena geográficamente el respaldo o copia de seguridad?				
9. Disponibilidad					
32.	¿Cómo se garantiza el servicio en línea a aquellos usuarios a los que no se extiende un allanamiento judicial?				
33.	¿Se asegura la disponibilidad de datos en caso de quiebra u otra pérdida de las instalaciones y cómo se define?				
10. Respuesta a incidentes					
34.	¿Existe un plan de respuesta a incidentes y cómo se define?				
35.	¿Hace el servicio seguimiento a los datos para determinar el alcance del incidente y los activos afectados?				
36.	¿Mantiene el servicio una copia forense de los datos acerca del incidente para procedimientos legales según lo necesite el consumidor? O, ¿el servicio proporciona datos acerca del incidente a los consumidores?				