Preguntas frecuentes sobre la seguridad de Adobe Creative Cloud para TI

La seguridad, la privacidad y el cumplimiento de la normativa de Creative Cloud son algunos de los temas para los que Adobe tiene que atender preguntas con mayor frecuencia. Las organizaciones que utilizan Creative Cloud tiene dudas respecto a la seguridad de sus datos y sobre si el acceso a los mismos es fiable. Con este documento, se pretende dar respuesta a las preguntas más frecuentes que plantea el personal dedicado a la seguridad en los departamentos de TI sobre este tipo de temas cuando se plantean utilizar Creative Cloud.

1 ¿Dónde se aloja Creative Cloud?

Creative Cloud está alojada en Amazon Web Services (AWS), lo cual incluye Amazon Elastic Compute Cloud (Amazon EC2) y Amazon Simple Storage Service (Amazon S3), en los Estados Unidos de América, UE y Asia Pacífico. AWS ofrece una plataforma segura para servicios de software que utilizan miles de empresas en todo el mundo. AWS proporciona servicios de acuerdo con las prácticas recomendadas en materia de seguridad, además obtiene certificaciones y lleva a cabo auditorías reconocidas en el sector (aws.amazon.com/security/). Esto implica que los miembros de Creative Cloud podrán disfrutar del compromiso continuado de Amazon respecto a las prácticas de seguridad dirigidas a los activos almacenados.

2 ¿Dónde se encuentran los datos de los clientes?

Los datos de los clientes se almacenan en Amazon S3 y Adobe elige la región física y los servidores donde se van almacenar los datos específicos de cada cliente. La replicación de datos para los objetos de datos en Amazon S3 se realiza en el clúster de la región donde se hayan almacenado los datos y no se replican en los clústeres de los centros de datos de otras regiones. Adobe implementa Creative Cloud en tres regiones: Estados Unidos de América, la Unión Europea y Asia Pacífico.

Ejemplo: De forma predeterminada, todos los datos de los clientes de Creative Cloud en la UE se almacenan en la nube del centro de datos de AWS en la UE y estos datos no se transferirán a centros de datos fuera de esta región.

3 ¿Quién controla los centros de datos de Creative Cloud?

En lo que respecta a las partes de Creative Cloud implementadas en AWS, es Amazon quien controla los componentes físicos. Con el fin de ayudar a los clientes a tener una mejor comprensión de los controles que AWS ha puesto en marcha y de su eficaz funcionamiento, AWS publica un informe sobre los controles implementados en organizaciones de servicios ("Service Organization Controls 1": SOC 1, Type 2) (aws.amazon.com/security/), con controles establecidos para Amazon EC2, Amazon S3 y Virtual Private Cloud (VPC), así como controles detallados sobre la seguridad física y del entorno. Estos controles se definen con un nivel de especificidad muy estricto que debería satisfacer la mayoría de las necesidades de los clientes.

4 ¿Permite Amazon a los clientes realizar visitas a los centros de datos de AWS?

No. Dado que los centros de datos de AWS alojan datos de múltiples clientes, AWS no permite que los clientes visiten los centros de datos, ya que esto expondría a muchos clientes al acceso físico por parte de terceros. Con el fin de satisfacer esta necesidad de los clientes, un auditor independiente y con la competencia debida valida la presencia y funcionamiento de los controles, lo cual forma parte del informe SOC 1, Type 2. Esta validación por parte de un tercero y de general aceptación aporta a los clientes una perspectiva independiente de la efectividad de los controles que se han puesto en marcha. Adobe ha firmado un acuerdo de confidencialidad con AWS y se puede obtener una copia del informe SOC 1 Type 2 (aws.amazon.com/security/). Las revisiones independientes para la seguridad física de los centros de datos forma asimismo parte de la auditoría de ISO 27001, de la evaluación PCI y del proceso de auditoría ITAR para AWS.

5 ¿Pueden los terceros tener acceso a los centros de datos de AWS?

AWS lleva un control estricto del acceso a los centros de datos, incluso en lo que respecta a sus empleados internos. Los terceros no dispondrán de acceso a los centros de datos de AWS salvo que cuenten con aprobación explícita por parte del director del centro de datos de AWS de acuerdo a la política de acceso de AWS. Consulte el informe SOC 1, Type 2 (aws.amazon.com/security/) para obtener información sobre los controles específicos respecto al acceso físico, autorización de acceso a los centros de datos y controles asociados.

6 ¿Quién es el responsable de aplicar revisiones?

Adobe es el responsable de aplicar revisiones en nuestros propios sistemas operativos (SO) invitados, software y aplicaciones que se ejecuten en AWS. AWS es el responsable de aplicar revisiones a los sistemas que admiten la prestación de los servicios de AWS, como son el hipervisor y los servicios de red. Esto se lleva a cabo según se especifica en la directiva de AWS y de acuerdo a la norma ISO 27001, NIST y los requisitos de PCI.

7 ¿Se supervisan o controlan las acciones con privilegios?
Los controles implementados limitan el acceso a sistemas y datos o bien, los datos se restringen y supervisan. Por otra parte, los datos de los clientes y, de forma predeterminada, las instancias del servidor se aíslan de otros clientes de manera lógica. Un auditor independiente supervisa el control del acceso de usuarios con privilegios a la infraestructura de AWS en las auditorías de SOC 1, ISO 27001, PCI, ITAR y FISMA para AWS.

8 ¿Se ocupa el proveedor de servicios en la nube de la amenaza que supone un acceso interno inapropiado a los datos y aplicaciones del cliente?
AWS proporciona un SOC 1 específico que se cubre en el informe SOC 1, Type 2 (aws.amazon.com/security/). Por otra parte, Adobe efectúa evaluaciones de riesgos periódicas sobre cómo se controla y supervisa el acceso interno.

9 ¿Cómo aísla Creative Cloud los datos de los clientes?
Todos los datos que almacena Adobe en nombre de los clientes disfrutan de una eficaz seguridad de aislamiento de inquilinos y capacidades de control. El almacenamiento de Creative Cloud utiliza Amazon S3, que proporciona controles avanzados de acceso a datos.

10 ¿Se ha implementado la segregación de clientes de forma segura?
El entorno de AWS es virtual y para varios inquilinos. AWS ha implementado procesos de gestión de la seguridad, controles PCI y otros controles de seguridad que se han diseñado para aislar a cada cliente de los demás. Los sistemas de AWS se han diseñado para evitar que los clientes puedan acceder al host o a instancias que no se les hubieran asignado mediante procesos de filtrado en el software de virtualización. Un asesor certificado para la seguridad (QSA, Qualified Security Assesor) independiente ha validado este tipo de arquitectura, la cual cumple todos los requisitos de PCI DSS 2.0 (aws.amazon.com/security/pci-dss-level-1-compliance-faqs/).

11 ¿Se ha encargado AWS de los puntos vulnerables conocidos del hipervisor?
Amazon EC2 utiliza actualmente una versión muy personalizada del hipervisor Xen. En procesos de evaluación y auditorías, los auditores independientes revisan regularmente la seguridad del hipervisor Xen de AWS. Consulte el documento sobre la seguridad de AWS (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) para obtener información sobre el hipervisor Xen y el aislamiento de instancias.

12 ¿Admiten los servicios el cifrado?
Creative Cloud cifra los datos en tránsito con SSL.

13 ¿Qué derechos tienen los proveedores de servicios en la nube sobre los datos de los clientes?
Los clientes de Creative Cloud ostentan el control y propiedad de sus datos. Consulte las Condiciones de uso de Adobe (www.adobe.com/go/gffooter_terms_of_use) y la Política de privacidad (www.adobe.com/privacy/policy.html) para obtener más información.

14 ¿Publica AWS los controles físicos y del entorno que realiza?
Sí. Los controles físicos y del entorno se describen específicamente en un informe SOC 1, Type 2. (aws.amazon.com/security/). Por otra parte, AWS cumple las normas ISO 27001 y FISMA, que exigen controles físicos y del entorno según las prácticas recomendadas.

15 ¿Los clientes pueden proteger y gestionar el acceso a Creative Cloud desde clientes como ordenadores y dispositivos móviles?
Sí. Creative Cloud permite a los clientes gestionar el acceso de cliente y remoto según sus propios requisitos.

16 ¿Permite AWS a los clientes proteger sus servidores virtuales?
Sí. Adobe ha implementado su propia arquitectura de seguridad en AWS, en función de las prácticas recomendadas del sector, lo cual incluye los 20 controles principales de SANS para la seguridad en Internet, Consensus Audit Guidelines, directrices NIST y normativa de Internet.

17 ¿Incluye AWS capacidades de gestión de identidades y acceso?
AWS dispone de un conjunto de ofertas para la gestión de identidades y acceso, lo cual permite a Adobe gestionar las identidades de los usuarios, asignar credenciales de seguridad, organizar a usuarios en grupos y gestionar los permisos de los usuarios de forma centralizada.

18 ¿Interrumpirá Adobe los sistemas de Creative Cloud para llevar a cabo tareas de mantenimiento?
Creative Cloud se ha implementado de tal forma que se elimina prácticamente el tiempo de inactividad. Los servicios deberían permanecer accesibles y disponibles durante las implementaciones nuevas gracias al uso de entornos alternativos y otros mecanismos de transición sin inactividad externa apreciable.

19 ¿Qué protección ofrece AWS frente ataques de denegación de servicio distribuido (DDoS)?
La red de AWS proporciona una protección importante respecto a la seguridad tradicional de la red. Consulte el documento sobre la seguridad de AWS (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) para obtener más información sobre este tema, lo cual incluye opiniones sobre DDoS.

20 ¿Dispone Adobe de un plan de continuidad empresarial para Creative Cloud?
AWS ofrece un programa de continuidad empresarial (media.amazonwebservices.com/AWS_Disaster_Recovery.pdf) y Creative Cloud se ha diseñado para su ejecución en múltiples regiones y para disponer de gran disponibilidad en diversas zonas o centros de datos. El diseño, arquitectura e implementación que ha utilizado Adobe confiere a Creative Cloud capacidad para utilizar una replicación de redundancia de datos y arquitecturas de implementación disponibles en diversas regiones o zonas.

21 ¿Especifica AWS la durabilidad de los datos?
Creative Cloud almacena datos en Amazon S3, lo cual aporta una infraestructura duradera de almacenamiento. Los objetos se almacenan de forma redundante en múltiples dispositivos en diversas instalaciones de una región de Amazon S3. Una vez se han almacenado los datos, Amazon S3 se encarga de detectar y reparar rápidamente cualquier pérdida de redundancia con el fin de mantener la durabilidad de los objetos. Asimismo, Amazon S3 verifica regularmente la integridad de los datos almacenados mediante sumas de comprobación. Si se detectan daños, se reparan mediante el uso de datos redundantes.

22 ¿Tiene previsto Adobe satisfacer los requisitos para el cumplimiento de la FISMA (Ley federal para la gestión de la seguridad de la información)?
Adobe no tiene planes inmediatos de obtener el certificado de cumplimiento de la FISMA (Ley federal para la gestión de la seguridad de la información) para Creative Cloud.

23 ¿Cumple Creative Cloud con la HIPAA?
Adobe no tiene previsto obtener la certificación de la HIPAA (Ley de transferencia y responsabilidad de seguros de salud de 1996) para Creative Cloud ya que no está destinada al procesamiento de historias médicas.

Referencias

Descripción general del documento sobre prácticas de seguridad de AWS, marzo 2013 (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf)

Documento sobre riesgos y cumplimiento de la normativa de AWS, enero 2013 (media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf)

Adobe

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
EE.UU.
www.adobe.com