Amazon Web Services: Riesgos y conformidad

Enero de 2016

(Consulte http://aws.amazon.com/compliance/aws-whitepapers/
para obtener acceso a la versión más actualizada de este documento)

Con este documento se pretende facilitar información destinada a ayudar a los clientes de AWS a integrar AWS con la estructura de control que tienen instalada para respaldar su entorno de TI. Este documento incluye un enfoque básico para evaluar los controles de AWS, además de información para ayudar a los clientes con la integración de los entornos de control. También se incluye información específica de AWS en relación con preguntas generales acerca de la conformidad de la cloud computing.

Índice

Información general sobre riesgos y conformidad

Habida cuenta de que AWS y sus clientes ejercen el control compartido del entorno de TI, ambas partes son responsables de la administración de dicho entorno. Por una parte, AWS es responsable de prestar sus servicios en una plataforma controlada y con un alto nivel de seguridad, así como de ofrecer un amplio abanico de características de seguridad que los clientes pueden utilizar. Por cuanto atañe a los clientes, su responsabilidad comprende configurar los entornos de TI de manera controlada y segura para satisfacer sus necesidades. Si bien los clientes no facilitan información a AWS acerca del uso y las configuraciones, en cambio, AWS sí informa a los clientes sobre el entorno de control y seguridad pertinente. Para ello, AWS se basa en:

- Obtener las certificaciones del sector y las acreditaciones independientes descritas en el presente documento
- Publicar información acerca de las prácticas de seguridad y control de AWS en documentos técnicos y en el contenido del sitio web
- Ofrecer certificados, informes y otra documentación directamente a los clientes de AWS en virtud de acuerdos de confidencialidad (según proceda)

Para obtener una descripción más detallada de la seguridad de AWS, visite el Centro de seguridad de AWS: https://aws.amazon.com/security/

Para obtener una descripción más detallada de la conformidad de AWS, visite el Centro de conformidad de AWS: https://aws.amazon.com/compliance/

Asimismo, en el documento técnico AWS Overview of Security Processes se abordan los controles generales de seguridad y la seguridad específica de los servicios de AWS.

Entorno de responsabilidad compartida

Al migrar la infraestructura de TI a los servicios de AWS, se crea un modelo de responsabilidad compartida entre el cliente y AWS. Este modelo compartido puede aliviar la carga operativa del cliente, ya que AWS opera, administra y controla los componentes del sistema operativo host y la capa de virtualización, a fin de ofrecer seguridad física en las instalaciones en las que operan los servicios. Por otra parte, el cliente asume la responsabilidad y la administración del sistema operativo invitado (incluidas las actualizaciones y los parches de seguridad), de cualquier otro software de aplicaciones asociadas y de la configuración del firewall del grupo de seguridad que ofrece AWS. Los clientes deben pensar detenidamente en los servicios que eligen, ya que las responsabilidades varían en función de los servicios que utilicen, de la integración de estos en su entorno de TI y de la legislación y los reglamentos aplicables. Los clientes pueden mejorar la seguridad o cumplir requisitos de conformidad más estrictos gracias a la utilización de aplicaciones tecnológicas como firewalls basados en host, prevención y detección de intrusiones basadas en host, cifrado y administración de claves. La naturaleza de esta responsabilidad compartida también ofrece la flexibilidad y la posibilidad de que el cliente pueda controlar la implementación de soluciones que satisfagan las necesidades de certificación específicas del sector.

Este modelo de responsabilidad compartida entre clientes y AWS también abarca los controles de TI. De la misma forma que AWS y sus clientes comparten la responsabilidad de operar el entorno de TI, también la comparten en lo referente a la administración, operación y verificación de los controles de TI. AWS puede ayudar a aliviar la carga que supone para los clientes operar los controles, administrando los controles asociados con la infraestructura física implementada en el entorno de AWS de cuya administración se encargaba el cliente anteriormente. Como la implementación de cada cliente se realiza de manera diferente en AWS, los clientes tienen la oportunidad de migrar a AWS la administración de determinados controles de TI para así obtener un entorno de control distribuido (nuevo). Los clientes pueden utilizar la documentación de control y conformidad de AWS disponible (se describe en la sección Certificaciones y acreditaciones independientes de AWS de este documento) para realizar sus procedimientos de evaluación y verificación de control según sea necesario.

En la siguiente sección se ofrece un enfoque acerca de cómo los clientes de AWS pueden evaluar y validar su entorno de control distribuido con eficacia.

Control exhaustivo de la conformidad

Como de costumbre, los clientes de AWS necesitan mantener un control adecuado de todo el entorno de control de TI con independencia de cómo se implemente la TI. Entre las principales prácticas destacan conocer los objetivos y los requisitos necesarios en materia de conformidad (a partir de las fuentes pertinentes), crear un entorno de control que satisfaga tales objetivos y requisitos, y conocer la validación necesaria conforme a la tolerancia de riesgos de la organización y la verificación de la eficacia operativa del entorno de control.
La implementación en la cloud de AWS ofrece a las compañías diferentes opciones para aplicar varios tipos de controles y diversos métodos de verificación.

A efectos de conseguir un sólido nivel de control y conformidad por parte del cliente, cabe adoptar el siguiente enfoque básico:

1. Revise la información disponible en AWS y toda la información adicional que proceda para conocer al máximo todo el entorno de TI y, a continuación, documente todos los requisitos de conformidad.
2. Diseñe e implemente los objetivos de control a efectos de satisfacer las necesidades empresariales en términos de conformidad.
3. Identifique y documente los controles que sean propiedad de terceros.
4. Compruebe que se cumplan todos los objetivos de control y que se han diseñado todos los controles principales y que estos operan con eficacia.

Enfocar el control de la conformidad de esta forma ayudará a las empresas a conocer mejor su entorno de control y a definir con claridad las actividades de verificación que cabe ejecutar.

Evaluación e integración de los controles de AWS

AWS ofrece a los clientes una gran variedad de información con respecto al entorno de control de TI a través de documentos técnicos, informes, certificaciones y otras acreditaciones independientes. Esta documentación ayuda a los clientes a conocer los controles existentes pertinentes para los servicios de AWS que utilizan y cómo estos controles han sido validados. Esta información también ayuda a los clientes a justificar y validar que los controles de su entorno de TI funcionan con eficacia.

Los auditores internos o externos suelen encargarse de validar el diseño y la eficacia operativa de los objetivos de control y los controles a través de revisiones de procesos y evaluación de pruebas. Por otra parte, el cliente o el auditor externo del cliente suelen realizar verificaciones y observaciones directas para validar los controles. En caso de que se utilicen proveedores de servicios, tales como AWS, las empresas solicitan y evalúan las certificaciones y acreditaciones independientes para obtener garantías razonables en relación con el diseño y la eficacia operativa de los controles y objetivos de control. Como resultado, si bien AWS puede administrar los controles clave del cliente, el entorno de control puede constituir una estructura unificada donde se tienen en cuenta todos los controles y donde también se verifica su eficacia operativa. Las acreditaciones independientes y las certificaciones de AWS no solo pueden ofrecer un nivel más alto de validación del entorno de control, sino que también pueden liberar a los clientes de tener que realizar determinadas tareas de validación del entorno de TI por sí mismos en la cloud de AWS.

Información acerca del control de TI de AWS

AWS facilita información acerca del control de TI a los clientes de las dos formas siguientes:

1. **Definición de controles específicos.** Los clientes de AWS pueden identificar los principales controles administrados por AWS. Los controles principales son de vital importancia para el entorno de control del cliente y se precisa de una acreditación externa sobre la eficacia operativa de estos controles con el fin de satisfacer los requisitos de conformidad, como la auditoría financiera anual. Para tal fin, AWS publica un amplio abanico de controles de TI específicos en su informe Service Organization Controls 1 (SOC 1), Tipo II. El informe SOC 1, denominado anteriormente el informe Declaración de Normas de Auditoría (SAS) N.º 70, Organizaciones de servicios, es un estándar de auditoría reconocido ampliamente desarrollado por el American Institute of Certified Public Accountants (AICPA) La auditoría SOC 1 es una auditoría exhaustiva utilizada para evaluar el diseño y la eficacia operativa de los objetivos y las actividades de control de AWS, entre otros, aquellos que comprenden parte de la infraestructura que AWS administra. La categoría "Tipo II" hace referencia al hecho de que cada uno de los controles descritos en el informe no solo se evalúa en términos de idoneidad del diseño, sino que los auditores externos también comprueban su eficacia operativa. Habida cuenta de la independencia y las competencias del auditor externo de AWS, los controles identificados en el informe aportan a los clientes un alto nivel de confianza en el entorno de control de AWS. El diseño y funcionamiento de los controles de AWS pueden considerarse eficaces para muchos fines de conformidad, entre otros, las auditorías de los estados financieros de la sección 404 de la Ley Sarbanes-Oxley (SOX). Otros organismos de certificación externos también pueden recurrir a los informes SOC 1, Tipo II (por ejemplo, los auditores de la ISO 27001 pueden solicitar un informe SOC 1, Tipo II, a fin de realizar las evaluaciones para los clientes).

Otras actividades de control específicas están relacionadas con el cumplimiento por parte de AWS de las normas del sector de tarjetas de pago (Payment Card Industry, PCI) y de la ley estadounidense Federal Information Security Management Act (FISMA). Tal y como se ha especificado anteriormente, AWS cumple las normas de seguridad del nivel FISMA Moderate y el estándar de seguridad de datos de PCI. Estas normas PCI y FISMA son muy prescriptivas y requieren una validación independiente de que AWS se atiene al estándar publicado.

2. **Conformidad con la norma de control general.** Si un cliente de AWS necesita que se cumplan una serie de objetivos de control, puede realizarse una evaluación de las certificaciones del sector de AWS. Con la certificación ISO 27001 de AWS, AWS cumple con una norma de seguridad amplia e integral, además de atenerse a las prácticas recomendadas relativas al mantenimiento de un entorno seguro. Con el estándar de seguridad de datos (Data Security Standard, DSS) del sector de tarjetas de pago (Payment Card Industry, PCI), AWS cumple con un conjunto de controles importantes para las empresas que procesan información sobre tarjetas de crédito. Habida cuenta de que AWS se atiene a las normas de la FISMA, AWS cumple un amplio abanico de controles específicos exigidos por organismos gubernamentales de EE. UU. La conformidad con estas normas generales ofrece a los clientes información exhaustiva sobre la naturaleza integral de los controles y los procesos de seguridad existentes, y puede tenerse en cuenta para la administración de la conformidad.

Regiones mundiales de AWS

Los centros de datos están agrupados en varias regiones del mundo. En el momento de redactar este documento hay doce regiones: EE.UU. Este (Norte de Virginia), EE.UU. Oeste (Oregón), EE.UU. Oeste (Norte de California), AWS GovCloud (EE.UU.) (Oregón), UE (Fráncfort), UE (Irlanda), Asia Pacífico (Seúl), Asia Pacífico (Singapur), Asia Pacífico (Tokio), Asia Pacífico (Sídney), China (Pekín) y América del Sur (São Paulo).

Programa de riesgos y conformidad de AWS

AWS facilita información acerca de su programa de riesgos y conformidad a fin de permitir a los clientes incorporar los controles de AWS en su estructura de control. Con esta información se pretende ayudar a los clientes a documentar una estructura completa de control en la que AWS constituya una parte importante de dicha estructura.

Administración de riesgos

El departamento de administración de AWS ha desarrollado un plan de negocio estratégico que comprende la identificación de riesgos y la ejecución de controles a efectos de mitigar o administrar los riesgos. Este departamento evalúa el plan al menos cada dos años. En este proceso, es preciso que el departamento de administración identifique los riesgos en sus ámbitos de responsabilidad, así como que adopte las medidas apropiadas destinadas a mitigar tales riesgos.

Asimismo, el entorno de control de AWS está sujeto a varias evaluaciones de riesgos internas y externas. Los equipos de Seguridad y conformidad de AWS han establecido un marco y políticas de seguridad de la información basados en el marco Control Objectives for Information and related Technology (COBIT, Objetivos de control para la información y tecnologías afines) y han integrado con eficacia el marco certificable ISO 27001 basándose en los controles de ISO 27002, los Principios de los servicios de confianza del American Institute of Certified Public Accountants (AICPA), el PCI DSS v3.1 y la revisión 3 de la Publicación 800-53 del National Institute of Standards and Technology (NIST, Instituto Nacional de Estándares y Tecnología) (Recommended Security Controls for Federal Information Systems). AWS se atiene en todo momento a la política de seguridad, ofrece capacitación a los empleados en materia de seguridad y realiza revisiones de la seguridad de las aplicaciones. En estas revisiones se evalúa la confidencialidad, la integridad y la disponibilidad de los datos, así como la conformidad con la política de seguridad de la información.

AWS Security analiza con regularidad todas las direcciones IP de punto de enlace de los servicios expuestas a Internet a fin de detectar vulnerabilidades (estos análisis no incluyen las instancias de los clientes). AWS Security notifica al respecto a las partes correspondientes para remediar todas las vulnerabilidades detectadas. Asimismo, empresas de seguridad independientes realizan con regularidad evaluaciones de amenazas de vulnerabilidades externas. Los resultados y las recomendaciones derivados de estas evaluaciones se clasifican y, además, se entregan a los equipos directivos de AWS. Estos análisis se realizan para comprobar el estado y la viabilidad de la infraestructura subyacente de AWS, por lo que no están pensados para reemplazar a los análisis de vulnerabilidades que realizan los clientes por su cuenta y que resultan necesarios para satisfacer sus requisitos de conformidad específicos. Los clientes pueden solicitar permiso para realizar análisis de la infraestructura de la cloud siempre que se limiten a las instancias del cliente y no infrinjan la Política de uso aceptable de AWS. La aprobación previa para realizar estos tipos de análisis se puede obtener enviando una solicitud a través del Formulario de Solicitud de Pruebas de Intrusión o Vulnerabilidades de AWS.

Entorno de control

AWS administra un entorno de control integral que comprende políticas, procesos y actividades de control que se benefician de varios aspectos del entorno de control global de Amazon. El objetivo de este entorno de control consiste en la entrega segura de ofertas de servicios de AWS. El entorno de control colectivo comprende al personal, los procesos y la tecnología necesarios para crear y mantener un entorno que respalde la eficacia operativa de la estructura de control de AWS. AWS ha integrado en su estructura de control los controles específicos de la cloud aplicables que han identificado los principales organismos del sector de cloud computing. AWS realiza un seguimiento de estos grupos del sector a fin de obtener ideas acerca de qué prácticas principales se pueden aplicar para facilitar aún más a los clientes la administración de su entorno de control.

El entorno de control en Amazon parte del estrato más alto de la empresa. Los altos cargos desempeñan funciones importantes a la hora de definir los valores principales y el tono de la empresa. A todos los empleados se les proporciona el código de conducta de la empresa y, además, realizan un proceso de capacitación periódica. Las auditorías de conformidad se realizan a fin de que los empleados puedan conocer y seguir las políticas establecidas.

La estructura organizativa de AWS ofrece una estructura de planificación, ejecución y control de las operaciones empresariales. Esta estructura organizativa asigna funciones y responsabilidades a fin de habilitar al personal adecuado, ofrecer eficacia en las operaciones y facilitar la segregación de funciones. La dirección también tiene una autoridad definida y líneas apropiadas para generar informes del personal clave. Los procesos de verificación de contratación de la empresa comprenden la capacitación, la experiencia profesional anterior y, en algunos casos, la comprobación de antecedentes de conformidad con la legislación y los reglamentos a efectos de que los empleados se ajusten al cargo del empleado y al nivel de acceso a las instalaciones de AWS. La empresa sigue un proceso de contratación estructurado para familiarizar a los nuevos empleados con las herramientas, los procesos, los sistemas, las políticas y los procedimientos de Amazon.

Seguridad de la información

AWS ha aplicado un programa formal de seguridad de la información diseñado para proteger la confidencialidad, la integridad y la disponibilidad de los sistemas y los datos de los clientes. AWS publica un documento técnico de seguridad que se encuentra disponible en el sitio web público en el que se explica cómo AWS puede ayudar a los clientes a proteger sus datos.

Certificaciones, programas e informes de AWS y acreditaciones independientes

AWS colabora con organismos de certificación externos y auditores independientes para ofrecer a los clientes información considerable acerca de las políticas, los procesos y los controles que establece y aplica AWS.

CJIS

AWS cumple el estándar Servicios de Información de la Justicia Penal (CJIS, Criminal Justice Information Services) del FBI. Firmamos acuerdos de seguridad de CJIS con nuestros clientes, entre los que se incluyen la realización de cualquier comprobación de antecedentes de los empleados necesaria de acuerdo con la **política de seguridad de CJIS**.

Los clientes de organismos de seguridad (y los socios que administran CJI) usan los servicios de AWS para mejorar la seguridad y la protección de los datos de CJI, a través de los servicios y características de seguridad avanzados de AWS, como el registro de actividades (**AWS CloudTrail**), el cifrado de datos en movimiento y en reposo (Cifrado de servidor de S3 con la opción de traer su propia clave), administración y protección exhaustivas de claves (AWS **Key Management Service** y **CloudHSM**) y administración integrada de permisos (administración de identidades federadas de IAM, autenticación multifactor).

AWS ha creado un **manual** de Servicios de Información de la Justicia Penal (CJIS) en forma de plantilla de plan de seguridad acorde con los ámbitos normativos de CJIS. Asimismo, se ha redactado un documento técnico de CJIS para guiar a los clientes en su viaje de adopción de la cloud.

Visite la página del centro de CJIS**: https://aws.amazon.com/compliance/cjis/**

CSA

En 2011, la Cloud Security Alliance (CSA) lanzó **STAR**, una iniciativa para promover la transparencia en las prácticas de seguridad de los proveedores de servicios en la cloud. STAR **(CSA Security, Trust & Assurance Registry)** es un registro de acceso público que documenta los controles de seguridad proporcionados por distintas ofertas de cloud computing, para ayudar a los usuarios a evaluar la seguridad de los proveedores de servicios en la cloud que utilizan actualmente o con los que tienen previsto trabajar. **AWS es un proveedor registrado en STAR de CSA** y ha completado el cuestionario Consensus Assessments Initiative Questionnaire (CAIQ) de Cloud Security Alliance (CSA). Este cuestionario CAIQ publicado por CSA ofrece una forma de hacer referencia a los controles de seguridad existentes en las ofertas de infraestructura como servicio de AWS y de documentarlos. El cuestionario CAIQ incluye 298 preguntas que un consumidor y un auditor de la cloud desearían preguntar a un proveedor de servicios en la cloud.

Consulte: **Apéndice A: Cuestionario Consensus Assessments Initiative Questionnaire de CSA v3.0.1**

Cyber Essentials Plus

Cyber Essentials Plus es un programa de certificaciones respaldado por el sector y por el gobierno del Reino Unido introducido en este país para ayudar a las organizaciones a demostrar la seguridad operativa frente a ciberataques comunes.

Esta certificación demuestra que los controles de referencia que implementa AWS mitigan el riesgo de las amenazas de Internet comunes, dentro del contexto de los "**10 pasos para la ciberseguridad**" del gobierno del Reino Unido. Es una certificación respaldada por el sector, incluida la Federación de Pequeñas Empresas, la Confederation of British Industry y una serie de compañías de seguros que ofrecen incentivos a las empresas que poseen esta certificación.

Cyber Essentials establece los controles técnicos necesarios; el marco de garantía asociado muestra cómo funciona el proceso de garantía independiente para la certificación Cyber Essentials Plus a través de una evaluación externa anual realizada por un asesor acreditado. Debido a la naturaleza regional de la certificación, el ámbito de esta certificación se limita la región UE (Irlanda).

SRG del DoD, niveles 2 y 4

El Modelo de seguridad en la cloud (SRG) del Departamento de Defensa (DoD) ofrece un proceso formalizado de evaluación y autorización para que los proveedores de servicios en la cloud (CSP) consigan una autorización provisional del DoD, que a su vez pueden utilizar los clientes del DoD. Las autorizaciones provisionales concedidas al amparo del SRG constituyen certificaciones reutilizables que atestiguan nuestra conformidad con los estándares del DoD, lo que reduce el tiempo que necesita un responsable del DoD para valorar y autorizar el funcionamiento de uno de sus sistemas en AWS. AWS posee actualmente autorizaciones provisionales en los niveles 2 y 4 del SRG.

Encontrará información adicional sobre las referencias de control de seguridad definidas para los **niveles 2, 4, 5 y 6 en: http://iase.disa.mil/cloud_security/Pages/index.aspx**.

Visite la página del centro de DoD**: https://aws.amazon.com/compliance/dod/**

FedRAMP SM

AWS es un proveedor de servicios en la cloud que cumple con el programa federal de administración de riesgos y autorizaciones (Federal Risk and Authorization Management Program, FedRAMP[sm]) de EE. UU. AWS ha completado las pruebas realizadas por una organización de evaluación independiente (3PAO, por sus siglas en inglés) acreditada por FedRAMP[sm] y el Departamento de Sanidad y Asuntos Sociales (HHS) de EE. UU. le ha otorgado dos títulos de autorización de agencia operativa (Agency Authority to Operate, ATO) tras demostrar su conformidad con los requisitos de FedRAMP[sm] con un nivel de impacto moderado. Todas las agencias del Gobierno de EE. UU. pueden usar los paquetes AWS Agency ATO almacenados en el repositorio de FedRAMP[sm] para evaluar a AWS respecto de sus aplicaciones y sus cargas de trabajo, para ofrecer autorizaciones de uso de AWS y para trasladar cargas de trabajo al entorno de AWS. Las dos Agency ATO de FedRAMP[sm] abarcan todas las regiones de EE. UU. (la región AWS GovCloud (EE.UU) y las regiones EE.UU Este y EE.UU Oeste de AWS). Los siguientes servicios se encuentran dentro de los límites de acreditación para las regiones indicadas anteriormente:

- Amazon Redshift. Amazon Redshift es un servicio rápido y totalmente administrado de almacenamiento de datos a escala de petabytes que permite analizar todos los datos empleando las herramientas de inteligencia empresarial existentes de forma sencilla y rentable.
- Amazon Elastic Compute Cloud (Amazon EC2). Amazon EC2 ofrece capacidad de cómputo de tamaño variable en la cloud. Se ha diseñado para facilitar a los desarrolladores recursos de computación escalables basados en la Web.
- Amazon Simple Storage Service (S3). Amazon S3 proporciona una sencilla interfaz de servicios web que puede utilizarse para almacenar y recuperar la cantidad de datos que desee, cuando desee y desde cualquier parte de la web.
- Amazon Virtual Private Cloud (VPC). Amazon VPC permite aprovisionar una sección de AWS aislada mediante lógica donde poder lanzar recursos de AWS en la red virtual que se defina.
- Amazon Elastic Block Store (EBS). Amazon EBS ofrece volúmenes de almacenamiento altamente disponibles, de confianza y predecibles que se pueden conectar a una instancia Amazon EC2 en ejecución y se pueden exponer como un dispositivo dentro de la instancia.
- AWS Identity and Access Management (IAM). IAM permite controlar de forma segura el acceso de los usuarios a servicios y recursos de AWS. Con IAM puede crear y administrar usuarios y grupos de AWS, así como utilizar permisos para permitir o denegar el acceso a los recursos de AWS.

Para obtener más información sobre la conformidad con FedRAMP[sm] de AWS, consulte las Preguntas más frecuentes sobre FedRAMP[sm] de AWS en: https://aws.amazon.com/compliance/fedramp/

FERPA

La Ley de derechos educativos de la familia y privacidad (Family Educational Rights and Privacy Act, FERPA) (20 U.S.C. § 1232g; 34 CFR parte 99) es una ley federal que protege la privacidad de los expedientes académicos de los estudiantes. La ley se aplica a todas las instituciones educativas que reciben fondos en virtud de un programa del Departamento de Educación de EE. UU. FERPA ofrece a los progenitores algunos derechos con respecto a los expedientes académicos de sus hijos. Estos derechos se transfieren al alumno cuando alcanza la edad de 18 años o asiste a una institución universitaria. Los estudiantes a los que se han transferido estos derechos son los "estudiantes cualificados".

AWS permite a las entidades cubiertas y a sus socios empresariales sujetos a la ley FERPA usar el entorno seguro de AWS para procesar, mantener y almacenar información académica protegida.

AWS ofrece además un **documento técnico dedicado a la FERPA** para los clientes que deseen informarse acerca de cómo pueden usar AWS para procesar y almacenar datos educativos.

En el **documento técnico sobre conformidad con la ley FERPA de AWS** se explica cómo las empresas pueden usar AWS para procesar sistemas que faciliten la conformidad con la ley FERPA: https://do.awsstatic.com/whitepapers/compliance/AWS_FERPA_Whitepaper.pdf

FIPS 140-2

La Publicación 140-2 del Federal Information Processing Standard (FIPS) es un estándar de seguridad del gobierno de EE .UU. que especifica los requisitos de seguridad para los módulos criptográficos que protegen información confidencial. Para ayudar a los clientes a cumplir los requisitos de FIPS 140-2, las terminaciones SSL de **AWS GovCloud (EE. UU.)** operan mediante el uso de hardware validado conforme a FIPS 140-2. AWS trabaja con los clientes de AWS GovCloud (EE.UU.) para facilitarles la información necesaria que les ayude a garantizar la conformidad cuando utilizan el **entorno de AWS GovCloud (EE.UU.)**.

FISMA y DIACAP

AWS permite a las agencias gubernamentales estadounidenses cumplir la ley estadounidense Federal Information Security Management Act (**FISMA**), relativa a la gestión de la seguridad de la información. La infraestructura de AWS ha sido evaluada por asesores independientes para diferentes sistemas gubernamentales como parte de su proceso de aprobación de propietarios de sistemas. Diversas organizaciones civiles y del Departamento de Defensa (DoD, por sus siglas en inglés) de Estados Unidos han logrado autorizaciones de seguridad para sistemas alojados en AWS, según el proceso Risk Management Framework (RMF), relativo a la administración de riesgos y definido en NIST 800-37, y al proceso DoD Information Assurance Certification and Accreditation Process (**DIACAP**) de certificación y acreditación de la calidad de la información.

GxP

GxP es un acrónimo que hace referencia a las regulaciones y directrices aplicables a organizaciones de ciencias de la salud que fabrican productos alimentarios y médicos, como medicinas, dispositivos médicos y aplicaciones de software médico. El propósito general de los requisitos de GxP es garantizar que los productos alimentarios y médicos son seguros para los consumidores y garantizar la integridad de los datos usados para tomar decisiones de seguridad relacionadas con estos productos.

AWS ofrece un **documento técnico sobre GxP** en el que se explica un enfoque exhaustivo sobre el uso de AWS para sistemas GxP. En este documento técnico se proporcionan directrices para usar los **productos de AWS en el contexto de GxP**. El contenido se ha desarrollado junto con clientes de dispositivos médicos y farmacéuticos de AWS, además de socios de software, que usan actualmente productos de AWS en sus sistemas GxP validados.

Para obtener más información sobre sistemas GxP en AWS **contacte con el equipo de AWS Sales and Business Development**.

Para obtener información adicional, consulte nuestras preguntas más frecuentes sobre la conformidad con GxP: https://aws.amazon.com/compliance/gxp-part-11-annex-11/

HIPAA

AWS permite que las entidades cubiertas y las empresas asociadas sujetas a la Ley estadounidense de portabilidad y responsabilidad de seguros médicos (Health Insurance Portability and Accountability Act, HIPAA) puedan beneficiarse del entorno seguro de AWS para procesar, mantener y almacenar información sanitaria confidencial, por lo que AWS suscribirá acuerdos de empresas asociadas con tales clientes. AWS ofrece además un documento técnico dedicado a la HIPAA para los clientes que deseen informarse acerca de cómo pueden aprovechar AWS para procesar y almacenar información sanitaria. En el documento técnico sobre diseño de la seguridad y conformidad con HIPAA en Amazon Web Services se explica cómo pueden utilizar AWS las empresas para procesar sistemas que faciliten la conformidad con HIPAA y Health Information Technology for Economic and Clinical Health (HITECH).

Los clientes pueden utilizar cualquier servicio de AWS en una cuenta designada como cuenta HIPAA, pero solo deben procesar, almacenar y transmitir información médica protegida (PHI) en los servicios que reúnan los requisitos de la HIPAA definidos en el BAA. En la actualidad, hay nueve servicios que cumplen los requisitos de la HIPAA, entre los que se incluyen los siguientes:

- Amazon DynamoDB
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Cloud Compute (EC2)
- Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon Glacier
- Amazon Redshift
- Amazon Relational Database Service (Amazon RDS) que usa solamente motores MySQL y Oracle
- Amazon Simple Storage Service (S3)

AWS sigue un programa de administración de riesgos basado en estándares para asegurarse de que los servicios que reúnen los requisitos de la HIPAA admiten expresamente los procesos de seguridad, control y administrativos necesarios en virtud de la HIPAA. El uso de estos servicios para almacenar y procesar información médica protegida (PHI) permite que nuestros clientes y AWS aborden las disposiciones de la HIPAA aplicables a nuestro modelo operativo basado en servicios públicos. AWS da prioridad a los servicios que reúnen los requisitos, y añade servicios nuevos, en función de la demanda de los clientes.

Para obtener información adicional, consulte nuestras preguntas más frecuentes sobre la conformidad con HIPAA: https://aws.amazon.com/compliance/hipaa-compliance/

Diseño de la seguridad y conformidad con HIPAA en Amazon Web Services: https://do.awsstatic.com/whitepapers/compliance/AWS_HIPAA_Compliance_Whitepaper.pdf

IRAP

El Programa de asesores registrados de seguridad de la información (IRAP, por sus siglas en inglés) permite a los clientes del gobierno australiano validar que se dispone de los controles adecuados y determinar el modelo de responsabilidad apropiado para abordar las necesidades del Manual de seguridad de la información (ISM) de la Dirección de Señales Australiana (ASD).

Amazon Web Services **ha realizado una evaluación independiente** que ha determinado que todos los controles de ISM aplicables relativos al procesamiento, almacenamiento y transmisión de datos sin clasificar (DLM) están implementados para la región de Sídney de AWS.

Preguntas más frecuentes sobre la conformidad con IRAP: https://aws.amazon.com/compliance/irap/

Para obtener más información, consulte: **Apéndice B: Conformidad de AWS con las consideraciones de seguridad de la cloud computing de la Dirección de Señales Australiana (ASD)**

ISO 9001

AWS ha obtenido la certificación ISO 9001. Esta certificación ayuda directamente a los clientes que desarrollan, migran y operan en la cloud de AWS sus sistemas de TI con control de calidad. Los clientes pueden utilizar los informes de conformidad de AWS para demostrar que disponen de sus propios programas ISO 9001 y programas de calidad específicos del sector, como GxP para las ciencias de la salud, ISO 13485 para dispositivos médicos, AS9100 para el sector aeroespacial e ISO/TS 16949 para el sector del automóvil. Los clientes de AWS que no poseen requisitos de sistema de calidad pueden beneficiarse de la seguridad y transparencia adicionales que proporciona la certificación ISO 9001.

La certificación ISO 9001 abarca el sistema de gestión de calidad en un ámbito especificado de servicios y regiones de AWS de operaciones (véase más abajo) y servicios, incluidos los siguientes:

- AWS CloudFormation
- AWS Cloud Hardware Security Model (HSM)
- Amazon CloudFront
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- Amazon DynamoDB
- Amazon EC2 VM Import/Export
- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Cloud Compute (EC2)
- Amazon EC2 Container Service (ECS)
- Amazon Elastic File System (EFS)
- Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- AWS Route 53
- Amazon SimpleDB
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- AWS Storage Gateway
- Amazon Simple Workflow Service (SWF)
- Amazon Virtual Private Cloud (VPC)

- AWS WAF - Firewall de aplicaciones web
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- La infraestructura física subyacente y el entorno de administración de AWS

La acreditación ISO 9001 de AWS abarca regiones de AWS, incluidas EE. UU. Este (Norte de Virginia), EE.UU. Oeste (Oregón), EE.UU. Oeste (Norte de California), AWS GovCloud (EE. UU.), América del Sur (São Paulo), UE (Irlanda), UE (Fráncfort), Asia Pacífico (Singapur), Asia Pacífico (Sídney) y Asia Pacífico (Tokio).

ISO 9001:2008 es un estándar global para administrar la calidad de productos y servicios. La norma 9001 describe un sistema de gestión de la calidad basado en ocho principios definidos por el Comité Técnico de Gestión y Garantía de la Calidad de la Organización Internacional de Normalización (ISO). Incluyen:

- Enfoque en los clientes
- Liderazgo
- Implicación de las personas
- Enfoque en el proceso
- Enfoque sistemático en la administración
- Mejora continua
- Enfoque realista en la toma de decisiones
- Relaciones de beneficio mutuo con los proveedores

La certificación ISO 9001 de AWS se puede descargar en:
https://d0.awsstatic.com/certifications/iso_9001_certification.pdf

AWS proporciona información adicional y preguntas frecuentes sobre su certificación ISO 9001 en:
https://aws.amazon.com/compliance/iso-9001-faqs/

ISO 27001

AWS ha obtenido la certificación ISO 27001 de nuestro sistema de gestión de la seguridad de la información (ISMS) que abarca la infraestructura, los centros de datos y los servicios de AWS, incluidos:

- AWS CloudFormation
- Amazon CloudFront
- AWS Cloudtrail
- AWS Directory Service
- Amazon DynamoDB
- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Cloud Compute (EC2)
- Amazon EC2 Container Service (ECS)
- AWS Direct Connect
- Amazon EC2 VM Import/Export
- AWS Cloud Hardware Security Model (HSM)
- Elastic Load Balancing (ELB)
- Amazon Elastic File System (EFS)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- AWS Identity and Access Management (IAM)

- AWS Key Management Service (KMS)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- AWS Route 53
- Amazon SimpleDB
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- AWS Storage Gateway
- Amazon Virtual Private Cloud (VPC)
- AWS WAF - Firewall de aplicaciones web
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- La infraestructura física subyacente (GovCloud incluido) y el entorno de administración de AWS

La ISO 27001/27002 es una norma de seguridad global muy extendida que fija los requisitos y las prácticas recomendadas para un enfoque sistemático en la administración de la información de empresas y clientes que se basa en evaluaciones de riesgo periódicas adecuadas a las siempre cambiantes amenazas posibles. Para poder obtener la certificación, la empresa debe mostrar que tiene un enfoque sistemático y en desarrollo continuo de la administración de los riesgos de seguridad de la información que afectan a la confidencialidad, integridad y disponibilidad de la información de la empresa y del cliente. Esta certificación refuerza el compromiso de Amazon de proporcionar información importante acerca de nuestros controles y nuestras prácticas de seguridad.

La acreditación ISO 27001 de AWS abarca regiones de AWS, incluidas EE. UU. Este (Norte de Virginia), EE.UU. Oeste (Oregón), EE.UU. Oeste (Norte de California), AWS GovCloud (EE. UU.), América del Sur (São Paulo), UE (Irlanda), UE (Fráncfort), Asia Pacífico (Singapur), Asia Pacífico (Sídney) y Asia Pacífico (Tokio).

La certificación ISO 27001 de AWS se puede descargar en:
https://d0.awsstatic.com/certifications/iso_27001_global_certification.pdf

AWS proporciona información adicional y preguntas frecuentes sobre su certificación ISO 27001 en:
https://aws.amazon.com/compliance/iso-27001-faqs/

ISO 27017

ISO 27017 es el código de conducta más reciente publicado por la Organización Internacional de Normalización (ISO). Ofrece pautas para implementar controles de seguridad asociados a los servicios de la cloud.

AWS ha obtenido la certificación ISO 27017 de nuestro sistema de administración de la seguridad de la información (ISMS) que abarca la infraestructura, los centros de datos y los servicios de AWS, incluidos:

- Amazon CloudFront
- Amazon DynamoDB
- Amazon EC2 Container Service (ECS)
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic File System (EFS)
- Amazon Elastic MapReduce (EMR)

- Amazon ElastiCache
- Amazon Glacier
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- Amazon SimpleDB
- Amazon Virtual Private Cloud (VPC)
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- AWS Storage Gateway
- AWS WAF (Firewall de aplicaciones web)
- Elastic Load Balancing
- VM Import/Export

La certificación ISO 27017 de AWS se puede descargar en:
https://do.awsstatic.com/certifications/iso_27017_certification.pdf

AWS proporciona información adicional y preguntas frecuentes sobre su certificación ISO 27017 en:
https://aws.amazon.com/compliance/iso-27017-faqs/

ISO 27018

ISO 27018 es el primer código de conducta internacional diseñado para proteger datos personales en la cloud. Se basa en la norma ISO de seguridad de la información 27002 y proporciona pautas de implementación sobre los controles ISO 27002 aplicables a la información de identificación personal (PII) en la cloud pública. Proporciona también una serie de controles adicionales y sus pautas correspondientes para abordar los requisitos de protección de PII en la cloud pública no recogidos en el conjunto de controles ISO 27002 existente.

AWS ha obtenido la certificación ISO 27018 de nuestro sistema de administración de la seguridad de la información (ISMS) que abarca la infraestructura, los centros de datos y los servicios de AWS, incluidos:

- Amazon CloudFront
- Amazon DynamoDB
- Amazon EC2 Container Service (ECS)
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic File System (EFS)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier

- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- Amazon SimpleDB
- Amazon Virtual Private Cloud (VPC)
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- AWS Storage Gateway
- AWS WAF (Firewall de aplicaciones web)
- Elastic Load Balancing
- VM Import/Export

La certificación ISO 27018 de AWS se puede descargar en:
https://d0.awsstatic.com/certifications/iso_27018_certification.pdf

AWS proporciona información adicional y preguntas frecuentes sobre su certificación ISO 27018 en:
https://aws.amazon.com/compliance/iso-27018-faqs/

ITAR

La región **AWS GovCloud (EE.UU.)** respalda la conformidad con el Reglamento estadounidense sobre el tráfico internacional de armas (**ITAR**). Dentro de la administración de un programa integral de conformidad con las regulaciones ITAR, las empresas sometidas a las regulaciones de exportación de ITAR deben controlar las exportaciones no intencionadas mediante la restricción del acceso a datos protegidos a ciudadanos de EE. UU. y limitar la ubicación física de esos datos al territorio de EE. UU. AWS GovCloud (EE.UU.) proporciona un entorno ubicado físicamente en EE. UU. y en el que el acceso por parte del personal de AWS se limita a ciudadanos de EE. UU., para permitir que las empresas que reúnan los requisitos exigidos transmitan, procesen y almacenen artículos y datos protegidos según las restricciones de ITAR. El entorno de AWS GovCloud (EE.UU.) ha sido auditado por una entidad externa independiente para validar que se aplican los controles adecuados a efectos de apoyar el cumplimiento de este requisito por los programas de conformidad de exportación de los clientes.

MPAA

La asociación Motion Picture Association of America (MPAA) ha establecido una serie de prácticas recomendadas para almacenar, procesar y ofrecer de forma segura medios y contenido protegidos (http://www.fightfilmtheft.org/facility-security- program.html). Las empresas de medios de comunicación utilizan estas prácticas recomendadas como mecanismo para valorar el riesgo y la seguridad de su contenido e infraestructura. AWS ha demostrado su conformidad con las prácticas recomendadas de MPAA, y la infraestructura de AWS ha superado todos los controles de infraestructura de MPAA aplicables. Aunque la MPAA no ofrece ninguna "certificación", los clientes del sector de los medios de comunicación pueden utilizar la documentación de AWS sobre MPAA para valorar y evaluar el riesgo que supone el entorno de AWS para el contenido de tipo MPAA.

Consulte la página del centro de conformidad con MPAA de AWS para obtener información adicional: https://aws.amazon.com/compliance/mpaa/

Certificación de MTCS de nivel 3

La **Seguridad en la cloud de varias capas (MTCS, por sus siglas en inglés)** es un estándar de administración de seguridad operativa de Singapur (SPRING SS 584:2013), que se basa en los estándares del Sistema de administración de la seguridad de la información (ISMS, Information Security Management System) de la norma ISO 27001/02. De acuerdo con la evaluación de la certificación, debemos hacer lo siguiente:

- Evaluar sistemáticamente los riesgos de seguridad de nuestra información y tener en cuenta el impacto de las vulnerabilidades y amenazas de la compañía
- Diseñar e implementar un paquete integral de controles de seguridad de la información y otras formas de administración de riesgos, con el fin de abordar los riesgos de seguridad de los diseños y de la compañía
- Adoptar un proceso de administración general para garantizar que los controles de seguridad de la información satisfagan nuestras necesidades de seguridad de la información constantemente

Visite la página del centro de MTCS en: https://aws.amazon.com/compliance/aws-multitiered-cloud-security-standard-certification/

NIST

En junio de 2015, el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) publicó las directrices **800-171**, "Final Guidelines for Protecting Sensitive Government Information Held by Contractors" (Pautas finales para proteger la información gubernamental confidencial mantenida por los contratistas). Estas directrices se aplican a la protección de información sin clasificar controlada (CUI) en sistemas no federales.

AWS ya se adhiere a estas directrices y los clientes pueden cumplir la norma NIST 800-171 inmediatamente. NIST 800-171 describe una serie de requisitos NIST 800-53, para los que AWS ya ha sido auditado en virtud del programa FedRAMP. La referencia de control de seguridad FedRAMP Moderate es más rigurosa que los requisitos recomendados establecidos en el capítulo 3 de 800-171, e incluye un gran número de controles de seguridad además de los exigidos por los sistemas FISMA Moderate que protegen los datos CUI. Encontrará una descripción detallada en la **Publicación especial de NIST 800-171**, a partir de la página D2 (que es la página 37 en el PDF).

PCI DSS Nivel 1

AWS alcanza el Nivel 1 conforme al Estándar de seguridad de datos (Data Security Standard, DSS) del sector de tarjetas de pago (Payment Card Industry, PCI). Los clientes pueden ejecutar aplicaciones en nuestra infraestructura tecnológica conforme al sector de PCI para el almacenamiento, procesamiento y transmisión de datos de tarjetas de crédito en la cloud. En febrero de 2013, el Consejo de estándares de seguridad de PCI publicó sus directrices de cloud computing conforme al estándar de seguridad de datos del sector de tarjetas de crédito PCI DSS Cloud Computing Guidelines. Estas directrices proporcionan a los clientes que administran entornos de datos de titulares de tarjeta instrucciones importantes para mantener los controles de PCI DSS en la cloud. AWS ha incorporado las directrices de cloud computing PCI DSS en el Paquete de conformidad con PCI de AWS para los clientes. El Paquete de conformidad con PCI de AWS incluye una confirmación de la conformidad de AWS con PCI (AoC, por sus siglas en inglés), que demuestra la validación satisfactoria de AWS conforme a los estándares aplicables a los proveedores de servicios de nivel 1 en la versión 3.1 de PCI DSS, además de un resumen de la responsabilidad de AWS respecto a PCI, donde se explica cómo se comparten las responsabilidades de conformidad entre AWS y nuestros clientes en la cloud.

Los servicios siguientes están incluidos en el ámbito de aplicación de PCI DSS Nivel 1:

- Auto Scaling
- AWS CloudFormation
- Amazon CloudFront
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- Amazon DynamoDB
- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon Glacier
- AWS Key Management Service (KMS)
- AWS Identity and Access Management (IAM)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon SimpleDB
- Amazon Simple Storage Service (S3)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Workflow Service SWF
- Amazon Virtual Private Cloud (VPC)
- La infraestructura física subyacente (GovCloud incluido) y el entorno de administración de AWS

El ámbito de aplicación más reciente de los servicios y las regiones para la certificación PCI DSS Nivel 1 de AWS está disponible en: https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

SOC 1/ISAE 3402

Amazon Web Services publica un informe Service Organization Controls 1 (SOC 1), Tipo II. La auditoría de este informe se realiza conforme a los estándares del American Institute of Certified Public Accountants (AICPA): AT 801 (anteriormente, SSAE 16) e International Standards for Assurance Engagements No. 3402 (ISAE 3402). Este informe regulado por dos estándares está pensado para cumplir una amplia variedad de requisitos de auditoría financiera de organismos de auditoría de EE. UU. e internacionales. La auditoría del informe SOC 1 certifica que los objetivos de control de AWS se diseñan de forma adecuada y que se definen los controles individuales para garantizar que los datos del cliente funcionan eficazmente. Este informe sustituye al informe de auditoría Statement on Auditing Standards No. 70 (SAS 70) Tipo II.

Aquí se especifican los objetivos de control de AWS conforme a SOC 1. En el mismo informe se identifican las actividades de control que respaldan cada uno de estos objetivos y los resultados que el auditor independiente ha obtenido de los procedimientos de pruebas de cada control.

Ámbito del objetivo	Descripción del objetivo
Organización de seguridad	Los controles ofrecen garantías razonables de que las políticas de seguridad de la información se han aplicado y comunicado en toda la organización.
Acceso de los usuarios empleados	Los controles ofrecen una garantía razonable de que se han establecido procedimientos para añadir, modificar y eliminar cuentas de usuarios empleados de Amazon de manera apropiada y oportuna, y que esos procedimientos se revisan de forma periódica.
Seguridad lógica	Los controles ofrecen una garantía razonable de que existen políticas y mecanismos para restringir adecuadamente el acceso no autorizado interno y externo a los datos, y el acceso a los datos de los clientes está separado debidamente de otros clientes.
Tratamiento seguro de los datos	Los controles ofrecen garantías razonables de que el tratamiento de los datos entre el punto de iniciación del cliente y una ubicación de almacenamiento de AWS se protege y asigna con precisión.
Protección de la seguridad física y del medio ambiente	Los controles ofrecen una garantía razonable de que el acceso físico a los centros de datos está restringido al personal autorizado y de que existen mecanismos para minimizar el efecto de un funcionamiento defectuoso o un desastre físico en las instalaciones de los centros de datos.
Administración de cambios	Los controles ofrecen garantías razonables de que se registran, autorizan, prueban, aprueban y documentan los cambios introducidos en los recursos de TI existentes, entre otros, cambios urgentes, no rutinarios y de configuración.
Redundancia, disponibilidad e integridad de los datos	Los controles ofrecen garantías razonables de que se mantiene la integridad de los datos en todas las fases, entre otras, en la transmisión, el almacenamiento y el procesamiento.
Administración de incidencias	Los controles ofrecen garantías razonables de que se registran, analizan y resuelven las incidencias del sistema.

Los informes SOC 1 están pensados para centrarse en los controles de una organización de servicios que pueden resultar relevantes para realizar una auditoría de los estados financieros de la entidad de un usuario. Habida cuenta de que AWS dispone de una amplia cartera de clientes, al igual que el uso de sus servicios, la aplicabilidad de los controles en los estados financieros de los clientes varía en función del cliente de que se trate. Por tanto, el informe SOC 1 de AWS está diseñado para abarcar controles clave específicos que probablemente resulten necesarios durante una auditoría financiera, así como para comprender un amplio abanico de controles generales de TI para aceptar una amplia variedad de escenarios de uso y auditoría. Esto permite a los clientes beneficiarse de la infraestructura de AWS para almacenar y procesar datos de vital importancia, incluidos aquellos que forman parte del proceso de generación de informes financieros. AWS evalúa periódicamente la selección de estos controles a fin de considerar la opinión de los clientes y el uso que estos hacen de este importante informe de auditoría.

El compromiso de AWS con el informe SOC 1 es continuo y AWS mantendrá el proceso de auditorías periódicas. El ámbito de aplicación del informe SOC 1 comprende:

- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- Amazon DynamoDB
- Amazon EC2 VM Import/Export
- Amazon Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon ElastiCache
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon Glacier
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon SimpleDB
- Amazon Simple Email Service (SES)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow (SWF)
- Amazon Simple Queue Service (SQS)
- AWS Storage Gateway
- Amazon Virtual Private Cloud (VPC)
- Amazon Workspaces

SOC 2

Además del informe SOC 1, AWS publica un informe Service Organization Controls 2 (SOC 2), Tipo II. El informe SOC 2, similar al SOC 1 en la evaluación de los controles, constituye un informe de confirmación que amplía la evaluación de los controles conforme a los criterios establecidos por los Principios de los servicios de confianza del American Institute of Certified Public Accountants (AICPA). Estos principios definen controles de prácticas principales relacionados con la seguridad, la disponibilidad, la integridad durante el procesamiento, la confidencialidad y la privacidad, aplicables a las organizaciones de servicios, como AWS. El informe AWS SOC 2 es una evaluación del diseño y eficacia operativa de los controles que cumplen los criterios de los principios de seguridad y disponibilidad estipulados en los Principios de los servicios de confianza del AICPA. Este informe proporciona una transparencia adicional respecto a la seguridad y disponibilidad de AWS de acuerdo con un estándar predefinido de prácticas principales del sector y demuestra el compromiso de AWS con la protección de los datos de los clientes. El ámbito de aplicación del informe SOC 2 comprende los mismos servicios que el informe SOC 1. Consulte la descripción de SOC 1 anterior para conocer los servicios que recaen dentro del ámbito de aplicación.

SOC 3

AWS publica un informe denominado Controles de las organizaciones de servicios 3 (SOC 3). El informe SOC 3 es un resumen del informe SOC 2 de AWS de disponibilidad pública. Incluye la opinión de un auditor externo acerca del funcionamiento de los controles (en función de los principios de seguridad del Instituto Americano de Auditores Públicos de Cuentas (AICPA por sus siglas en inglés), incluidos en el informe SOC 2), la declaración del departamento de administración de AWS relativa a la eficacia de los controles e información general acerca de la infraestructura y los servicios de AWS. El informe AWS SOC 3 incluye todos los centros de datos de AWS en todo el mundo que ofrecen los servicios prestados. Es un magnífico recurso para que los clientes validen que AWS cuenta con la garantía de auditores externos sin pasar por el proceso de solicitar un informe SOC 2. El ámbito de aplicación del informe SOC 3 comprende los mismos servicios que el informe SOC 1. Consulte la descripción de SOC 1 anterior para conocer los servicios que recaen dentro del ámbito de aplicación. Consulte aquí el informe SOC 3 de AWS.

Preguntas clave sobre conformidad y AWS

En esta sección se incluyen preguntas generales acerca de la conformidad de la cloud computing específicas de AWS. Estas preguntas comunes acerca de la conformidad pueden resultar interesantes para evaluar y operar un entorno de cloud computing y, además, pueden facilitar las tareas de administración de control de los clientes de AWS.

Ref.	Pregunta sobre cloud computing	Información de AWS
1	Titularidad del control. ¿De quién es la titularidad de los controles de la infraestructura implementada en la cloud?	Por cuanto atañe a la parte que se implementa en AWS, AWS controla los componentes físicos de dicha tecnología. El cliente tiene la titularidad y el control de todo lo demás, incluido el control de los puntos de conexión y las transmisiones. Para ayudar a los clientes a comprender mejor los controles que aplicamos y la eficacia con la que operan, publicamos un informe SOC 1, Tipo II, con los controles definidos para EC2, S3 y VPC, así como controles detallados de carácter ambiental y para la seguridad física. Estos controles se definen con un alto nivel de especificidad que debe satisfacer la mayoría de las necesidades de los clientes. Los clientes de AWS que hayan firmado un acuerdo de confidencialidad con AWS pueden solicitar una copia del informe SOC 1, Tipo II.
2	Auditoría de TI. ¿Cómo puede realizarse la auditoría del proveedor de la cloud?	El cliente es responsable de auditar la mayoría de las capas y los controles que van más allá de los controles físicos. La definición de los controles lógicos y físicos definidos por AWS está documentada en el informe SOC 1, Tipo II, y el informe se encuentra disponible para que los equipos de auditoría y conformidad puedan revisarlo. La certificación ISO 27001 y otras certificaciones de AWS también se encuentran disponibles para su revisión por parte de los auditores.
3	Conformidad con Sarbanes-Oxley. ¿Cómo se consigue la conformidad con SOX si los sistemas comprendidos en el ámbito de aplicación se implementan en el entorno del proveedor de la cloud?	Si un cliente procesa información financiera en la cloud de AWS, los auditores del cliente pueden determinar si algunos sistemas de AWS recaen dentro del ámbito de aplicación a efectos de cumplimiento de las disposiciones de Sarbanes-Oxley (SOX). Los auditores del cliente pueden extraer su propia conclusión acerca de la aplicabilidad de SOX. Habida cuenta de que el cliente es responsable de administrar la mayoría de los controles de acceso lógicos, es el más apto para determinar si las actividades de control que lleva a cabo cumplen las normas correspondientes. Si los auditores de SOX solicitan información específica sobre los controles físicos de AWS, pueden remitirse al informe SOC 1, Tipo II, de AWS, donde se detallan los controles que ofrece AWS.
4	Conformidad con HIPAA. ¿Es posible cumplir los requisitos de conformidad de la ley HIPAA al realizar la implementación en el entorno del proveedor de la cloud?	Las disposiciones de la HIPAA se aplican al cliente de AWS y es el cliente el encargado de controlar que así sea. La plataforma de AWS admite la implementación de soluciones que satisfacen los requisitos de certificación específicos del sector, como la HIPAA. Los clientes pueden usar los servicios de AWS para mantener un nivel de seguridad equivalente o superior al que se necesita para proteger registros de estado electrónicos. Los clientes han creado aplicaciones sanitarias que cumplen con las normas de seguridad y privacidad HIPAA en AWS. AWS ofrece información adicional en su sitio web acerca de la conformidad con la HIPAA, incluido un documento técnico acerca de este tema.

Ref.	Pregunta sobre cloud computing	Información de AWS
5	Conformidad con GLBA ¿Es posible cumplir los requisitos de la certificación GLBA al realizar la implementación en el entorno del proveedor de la cloud?	La mayoría de los requisitos de la GLBA los controla el cliente de AWS. AWS ofrece medios para que los clientes protejan los datos, administren los permisos y creen aplicaciones compatibles con la GLBA en la infraestructura de AWS. Si los clientes precisan de garantías específicas de que los controles de seguridad físicos funcionan con eficacia, pueden consultar el informe SOC 1, Tipo II, de AWS según corresponda.
6	Conformidad con el reglamento federal. ¿Es posible que un organismo gubernamental de los Estados Unidos cumpla los reglamentos de seguridad y privacidad al realizar la implementación en el entorno del proveedor de la cloud?	Las agencias gubernamentales estadounidenses pueden cumplir una serie de estándares de conformidad, incluida la ley estadounidense Federal Information Security Management Act (FISMA) relativa a la administración de la seguridad de la información de 2002, el Federal Risk and Authorization Management Program (FedRAMP) para la administración de riesgos y autorizaciones, la Publicación 140-2 del Federal Information Processing Standard (FIPS) y el Reglamento estadounidense sobre el tráfico internacional de armas (ITAR). También se pueden cumplir otras leyes y reglamentos en función de los requisitos previstos en la legislación aplicable.
7	Ubicación de los datos. ¿Dónde se alojan los datos de los clientes?	Los clientes de AWS designan en qué región física se ubicarán sus datos y servidores. La replicación de los datos para los objetos de datos de S3 se realiza dentro del clúster regional en el que se almacenan los datos, y la replicación no se realiza en otros clústeres del centro de datos de otras regiones. Los clientes de AWS designan en qué región física se ubicarán sus datos y servidores. AWS no moverá el contenido de los clientes desde las regiones seleccionadas sin notificárselo, a menos que resulte necesario a efectos de cumplir la legislación o por petición de organismos gubernamentales. En el momento de redactar este documento hay doce regiones: EE.UU. Este (Norte de Virginia), EE.UU. Oeste (Oregón), EE.UU. Oeste (Norte de California), AWS GovCloud (EE.UU.) (Oregón), UE (Fráncfort), UE (Irlanda), Asia Pacífico (Seúl), Asia Pacífico (Singapur), Asia Pacífico (Tokio), Asia Pacífico (Sídney), China (Pekín) y América del Sur (São Paulo).
8	Exhibición de documentos electrónicos. ¿El proveedor de la cloud satisface las necesidades de los clientes a fin de cumplir los requisitos y los procedimientos de exhibición de documentos electrónicos?	AWS ofrece la infraestructura, y los clientes administrar todo lo demás, como el sistema operativo, la configuración de red y las aplicaciones instaladas. Los clientes son responsables de responder según proceda a los procedimientos legales que impliquen la identificación, la recopilación, el procesamiento, el análisis y la elaboración de los documentos electrónicos que almacenan o procesan con AWS. Previa solicitud, AWS puede colaborar con los clientes que requieran la asistencia de AWS en procedimientos legales.

Ref.	Pregunta sobre cloud computing	Información de AWS
9	Visitas al centro de datos. ¿El proveedor de la cloud permite que los clientes visiten en centro de datos?	No. Como nuestros centros de datos alojan muchos clientes, AWS no permite que estos realicen visitas a los centros de datos, ya que ello supondría que muchos clientes tendrían acceso físico a información de terceros. A fin de satisfacer esta necesidad del cliente, un auditor independiente y competente valida la existencia y la operación de los controles como parte de nuestro informe SOC 1, Tipo II. Esta validación de terceros ampliamente aceptada ofrece a los clientes un punto de vista independiente de la eficacia de los controles existentes. Los clientes de AWS que hayan firmado un acuerdo de confidencialidad con AWS pueden solicitar una copia del informe SOC 1, Tipo II. Las revisiones independientes de la seguridad física de los centros de datos forman parte también de la auditoría ISO 27001, la evaluación de PCI, la auditoría de ITAR y los programas de prueba de FedRAMP[sm].
10	Acceso de terceros. ¿Se permite el acceso de terceros a los centros de datos del proveedor de la cloud?	AWS controla de manera estricta el acceso a los centros de datos, incluso para empleados internos. No se proporciona acceso a terceros a los centros de datos de AWS salvo cuando lo aprueba de forma explícita el director del centro de datos de AWS correspondiente de acuerdo con la política de acceso de AWS. Consulte el informe SOC 1 Tipo II para conocer los controles específicos relacionados con el acceso físico, la autorización de acceso a los centros de datos y otros controles relacionados.
11	Acciones privilegiadas. ¿Las acciones privilegiadas se supervisan y controlan?	Los controles existentes limitan el acceso a sistemas y datos, además de estipular que el acceso a los sistemas o datos se restrinja y monitoree. Asimismo, los datos de los clientes y las instancias de servidor se aíslan de forma lógica de otros clientes de manera predeterminada. Un auditor independiente examina el control de acceso de usuarios privilegiados en el marco de las auditorías de SOC 1, ISO 27001, PCI, ITAR y FedRAMP[sm] de AWS.
12	Acceso confidencial. ¿El proveedor de la cloud aborda las amenazas del acceso confidencial inapropiado a las aplicaciones y los datos de los clientes?	AWS ofrece controles SOC 1 específicos para abordar la amenaza del acceso confidencial inapropiado, y las iniciativas de conformidad y certificación públicas tratadas en este documento abordan el acceso confidencial. Todas las certificaciones y acreditaciones independientes evalúan los controles lógicos de detección y prevención de acceso. Asimismo, las evaluaciones de riesgo periódicas se centran en la forma de controlar y monitorear el acceso confidencial.

Ref.	Pregunta sobre cloud computing	Información de AWS
13	Varias organizaciones. ¿La segregación de clientes se aplica de forma segura?	El entorno de AWS es un entorno virtualizado multiempresa. AWS ha aplicado procesos de administración de seguridad, controles PCI y otros controles de seguridad diseñados para aislar a cada cliente de los demás. Los sistemas de AWS están diseñados para impedir que los clientes accedan a las instancias o a los hosts físicos que no tengan asignados mediante la aplicación de filtros a través del software de virtualización. Un asesor de seguridad cualificado (QSA) de PCI independiente ha validado esta arquitectura, y demostró su conformidad con todos los requisitos de la versión 3.1 de PCI DSS publicada en abril de 2015. Tenga en cuenta que AWS también tiene opciones de una sola organización. Las instancias dedicadas son instancias Amazon EC2 lanzadas en Amazon Virtual Private Cloud (Amazon VPC) que ejecutan hardware dedicado a un único cliente. Las instancias dedicadas le permiten obtener el máximo provecho de los beneficios de Amazon VPC y de la cloud de AWS, a la vez que aísla las instancias de computación de Amazon EC2 en el nivel de hardware.
14	Vulnerabilidades del hipervisor. ¿El proveedor de la cloud ha abordado vulnerabilidades conocidas del hipervisor?	Amazon EC2 actualmente utiliza una versión bastante personalizada del hipervisor Xen. Los equipos de intrusión internos y externos evalúan regularmente el hipervisor para detectar las vulnerabilidades nuevas y existentes y los vectores de ataque. Este hipervisor está perfectamente adaptado para mantener un fuerte aislamiento entre las máquinas virtuales invitadas. Durante las evaluaciones y auditorías, los auditores independientes evalúan con regularidad la seguridad del hipervisor Xen de AWS. Consulte el documento técnico de seguridad de AWS para obtener información adicional acerca del aislamiento de instancias y del hipervisor Xen.
15	Administración de vulnerabilidades. ¿Se aplican correctamente los parches de los sistemas?	AWS es responsable de aplicar parches de los sistemas que respalden la prestación del servicio a los clientes, como el hipervisor y los servicios de redes. Esto se hace de conformidad con la política de AWS y con los requisitos de ISO 27001, NIST y PCI. Los clientes controlan los sistemas operativos invitados, el software y las aplicaciones con los que cuentan y, por tanto, también son responsables de aplicar los parches de sus propios sistemas.
16	Cifrado. ¿Los servicios prestados admiten el cifrado?	Sí. AWS permite a los clientes utilizar sus propios mecanismos de cifrado prácticamente para todos los servicios, entre otros, S3, EBS, SimpleDB y EC2. Los túneles IPSec con VPC también están cifrados. Amazon S3 también ofrece a los clientes la opción de utilizar el cifrado del servidor. Además, los clientes también pueden utilizar tecnologías de cifrado de terceros. Consulte el documento técnico de seguridad de AWS para obtener más información.

Ref.	Pregunta sobre cloud computing	Información de AWS
17	Titularidad de los datos. ¿Qué derechos tiene el proveedor de la cloud sobre los datos de los clientes?	Los clientes de AWS mantienen el control y la propiedad de sus datos. AWS ofrece un alto nivel de protección de la privacidad de los clientes, por lo que está alerta a la hora de determinar qué requisitos de conformidad con las leyes debemos cumplir. AWS no duda en impugnar las órdenes de las autoridades si considera que carecen de fundamentos sólidos.
18	Aislamiento de los datos. ¿El proveedor de la cloud aísla correctamente los datos de los clientes?	Todos los datos almacenados por AWS en nombre de los clientes tienen capacidades sólidas de control y seguridad de aislamiento de organizaciones. Amazon S3 ofrece controles avanzados de acceso a los datos. Consulte el documento técnico de seguridad de AWS para obtener información adicional acerca de la seguridad específica de los servicios de datos.
19	Servicios compuestos. ¿El proveedor de la cloud comparte su servicio con los servicios de la cloud de otros proveedores?	AWS no recurre a ningún otro proveedor de la cloud para proporcionar servicios de AWS a los clientes.
20	Controles ambientales y físicos. ¿El proveedor de la cloud especificado opera estos controles?	Sí. Se describen específicamente en el informe SOC 1, Tipo II. Además, otras certificaciones de AWS como ISO 27001 y FedRAMPsm requieren que los controles físicos y de protección del medio ambiente sean prácticas recomendadas.
21	Protección por parte del cliente. ¿El proveedor de la cloud permite a los clientes proteger y administrar el acceso desde clientes, como equipos y dispositivos móviles?	Sí. AWS permite a los clientes administrar las aplicaciones cliente y móviles conforme a sus propias necesidades.
22	Seguridad del servidor. ¿El proveedor de la cloud permite a los clientes proteger sus servidores virtuales?	Sí. AWS permite a los clientes aplicar su propia arquitectura de seguridad. Consulte el documento técnico de seguridad de AWS para obtener más detalles acerca de la seguridad del servidor y de la red.
23	Identity and Access Management. ¿El servicio incluye las funciones de IAM?	AWS dispone de un conjunto de servicios de administración de identidad y acceso, que permiten a los clientes administrar las identidades de los usuarios, asignar credenciales de seguridad, organizar a los usuarios en grupos y administrar los permisos de los usuarios de forma centralizada. Consulte el sitio web de AWS para obtener más información.
24	Interrupciones de mantenimiento previstas. ¿El proveedor especifica cuándo se interrumpirán los sistemas para realizar el mantenimiento?	AWS no necesita interrumpir los sistemas para realizar tareas regulares de mantenimiento ni para aplicar parches a los mismos. La aplicación de parches del sistema y el mantenimiento de AWS no suelen repercutir en los clientes. El cliente es el encargado de controlar el mantenimiento de las instancias.

Ref.	Pregunta sobre cloud computing	Información de AWS
25	Capacidad de escalado. ¿El proveedor permite a los clientes escalar más allá del acuerdo original?	La cloud de AWS es distribuida, muy segura y resistente, por lo que ofrece a los clientes una gran capacidad de escalado. Los clientes pueden aumentar o reducir el escalado y pagar solo por lo que utilicen.
26	Disponibilidad del servicio. ¿El proveedor confirma un alto nivel de disponibilidad?	AWS confirma altos niveles de disponibilidad en sus acuerdos de nivel de servicios (SLA). Por ejemplo, Amazon EC2 garantiza un porcentaje anual de tiempo de actividad de al menos el 99,95 % durante el año de servicio. Amazon S3 garantiza un porcentaje de tiempo de actividad mensual de al menos el 99,9 %. Se ofrecen créditos de servicio para los casos en que no se cumplan estas métricas de disponibilidad.
27	Ataques de denegación de servicio distribuido (DDoS). ¿Cómo protege el proveedor su servicio frente a los ataques DDoS?	La red de AWS ofrece protección de alto nivel frente a los problemas tradicionales de seguridad de la red, y el cliente puede aplicar medidas adicionales de protección. Consulte el documento técnico de seguridad de AWS para obtener más información acerca de este tema, incluidos los detalles relativos a los ataques DDoS.
28	Portabilidad de los datos. ¿Se pueden exportar los datos almacenados con un proveedor del servicio por petición del cliente?	AWS permite que los clientes extraigan y añadan datos en los servicios de almacenamiento de AWS. El servicio AWS Import/Export para S3 acelera la transferencia de grandes volúmenes de datos desde y hacia AWS utilizando dispositivos de almacenamiento portátiles.
29	Continuidad del negocio del proveedor del servicio. ¿El proveedor del servicio aplica un programa de continuidad del negocio?	AWS aplica un programa de continuidad del negocio. Puede encontrar información detallada en este sentido en el documento técnico de seguridad de AWS.
30	Continuidad de negocio del cliente. ¿El proveedor del servicio permite que los clientes apliquen un plan de continuidad del negocio?	AWS ofrece a los clientes la posibilidad de aplicar un sólido plan de continuidad, incluida la utilización de backups frecuentes de las instancias del servidor, replicación de redundancia de los datos y arquitecturas de implementación en varias zonas de disponibilidad y regiones.
31	Durabilidad de los datos. ¿El servicio especifica la durabilidad de los datos?	Amazon S3 ofrece una infraestructura de almacenamiento que presenta elevados niveles de durabilidad. Los objetos se almacenan de forma redundante en varios dispositivos de diversas instalaciones dentro de una región de Amazon S3. Una vez almacenados, Amazon S3 mantiene la durabilidad de los objetos detectando y reparando rápidamente cualquier pérdida de redundancia. Del mismo modo, Amazon S3 comprueba de forma regular la integridad de los datos almacenados mediante sumas de comprobación. Si se detecta algún tipo de daño en los objetos, se reparan utilizando los datos redundantes. En caso de los datos almacenados en S3, el servicio está diseñado para ofrecer una durabilidad del 99,999999999 % y una disponibilidad de los objetos del 99,99 % durante un año concreto.

Ref.	Pregunta sobre cloud computing	Información de AWS
32	Backups. ¿El servicio ofrece backups en cintas?	AWS permite a los clientes realizar sus propios backups en cintas con su propio proveedor de servicios de backup en cinta. No obstante, AWS no ofrece el servicio de backup en cinta. El servicio de Amazon S3 está diseñado para abordar la probabilidad de que se produzcan pérdidas de datos con un porcentaje próximo a cero, y la durabilidad equivalente de copias en varios sitios de los objetos de datos se consigue con la redundancia del almacenamiento de los datos. Para obtener información acerca de la redundancia y la durabilidad de los datos, consulte el sitio web de AWS.
33	Subidas de precios. ¿El proveedor del servicio sube los precios de manera repentina?	A AWS le avala un historial de reducciones frecuentes de los precios a medida que se reducen los costos por la prestación de los servicios a lo largo del tiempo. AWS ha reducido los precios sistemáticamente durante los últimos años.
34	Sostenibilidad. ¿La empresa del proveedor del servicio tiene potencial para la sostenibilidad a largo plazo?	AWS es un proveedor líder de la cloud y, además, se trata de una estrategia empresarial a largo plazo de Amazon.com. AWS cuenta con un amplio potencial de sostenibilidad a largo plazo.

Contacto de AWS

Los clientes pueden ponerse en contacto con el equipo de AWS Sales and Business Development para solicitar los informes y las certificaciones de auditores externos y para solicitar información adicional acerca de la conformidad de AWS. El representante remitirá a los clientes al equipo adecuado en función de la naturaleza de la consulta. Para obtener más información sobre la conformidad de AWS, visite el sitio de conformidad de AWS o envíe sus preguntas directamente a awscompliance@amazon.com.

Apéndice A: Cuestionario Consensus Assessments Initiative Questionnaire de CSA v3.0.1

Cloud Security Alliance (CSA) es una "organización sin ánimo de lucro con la misión de promover el uso de prácticas recomendadas para ofrecer garantías de seguridad en el ámbito de la cloud computing, así como de ofrecer información acerca de los usos de la cloud computing a efectos de ayudar a proteger todas las formas de computación". [Referencia **https://cloudsecurityalliance.org/about/**] Un amplio abanico de profesionales, empresas y asociaciones del ámbito de la seguridad participan en esta organización para conseguir esta misión.

El cuestionario Consensus Assessments Initiative Questionnaire de CSA incluye una serie de preguntas que la CSA prevé que un usuario o un auditor de la cloud podría plantearse acerca de un proveedor de la cloud. Contiene una serie de preguntas acerca de la seguridad, el control y los procesos que pueden utilizarse para una amplia variedad de usos, entre otros, para evaluar la seguridad y seleccionar al proveedor de la cloud. AWS ha completado este cuestionario con las siguientes respuestas.

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
Seguridad de aplicaciones e interfaces *Seguridad de aplicaciones*	AIS-01.1	¿Utiliza normas del sector (puntos de referencia de Build Security in Maturity Model [BSIMM], la estructura de proveedor de tecnología de confianza Open Group ACS Trusted Technology Provider Framework, NIST, etc.) para aportar seguridad a los sistemas y al ciclo de vida de desarrollo de software (SDLC)?	El ciclo de vida de desarrollo de sistemas de AWS incorpora las prácticas recomendadas del sector, que incluyen las revisiones formales de diseño de AWS Security Team, el modelado de amenazas y la realización de una evaluación de riesgos. Consulte el documento técnico de información general sobre los procesos de seguridad de AWS para obtener información adicional. AWS cuenta con procedimientos para administrar nuevos desarrollos de recursos. Consulte la norma ISO 27001, anexo A, dominio 14, para obtener información adicional. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
	AIS-01.2	¿Utiliza una herramienta de análisis de código abierto automatizada para detectar los defectos de seguridad antes de la producción?	
	AIS-01.3	¿Utiliza una herramienta de análisis de código abierto manual para detectar los defectos de seguridad antes de la producción?	
	AIS-01.4	¿Verifica si todos los proveedores de software se atienen a las normas del sector en relación con la seguridad del ciclo de vida de desarrollo de sistemas y software (SDLC)?	
	AIS-01.5	(Solo para SaaS) ¿Revisa sus aplicaciones para detectar vulnerabilidades de seguridad y abordar todos los problemas antes de implementar las aplicaciones en producción?	

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
Seguridad de aplicaciones e interfaces *Requisitos de acceso de los clientes*	AIS-02.1	¿Se abordan y tratan todos los requisitos normativos, contractuales y de seguridad identificados para el acceso de los clientes por contrato antes de concederles acceso a los datos, los recursos y los sistemas de información?	Los clientes de AWS tienen la responsabilidad de garantizar que el uso que hacen de AWS se atiene a los reglamentos y las leyes aplicables. AWS informa acerca de su entorno de control y seguridad a los clientes a través de acreditaciones independientes y certificaciones del sector y documentos técnicos (disponibles en http://aws.amazon.com/compliance), además de ofrecer directamente a los clientes de AWS certificaciones, informes y otra documentación relevante.
	AIS-02.2	¿Están definidos y documentados todos los requisitos y niveles de confianza de acceso de los clientes?	
Seguridad de aplicaciones e interfaces *Integridad de los datos*	AIS-03.1	¿Se ejecutan rutinas de integridad de entrada y salida de los datos (es decir, comprobaciones de edición y reconciliación) para las bases de datos y las interfaces de la aplicación a fin de prevenir los errores de procesamiento manual o sistemático o la corrupción de los datos?	Los controles de integridad de los datos de AWS que se describen en los informes SOC de AWS ilustran los controles de integridad de los datos mantenidos en todas las fases, entre otras, la transmisión, el almacenamiento y el procesamiento. Además, consulte la norma ISO 27001, anexo A, dominio 14, para obtener información adicional. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
Seguridad de aplicaciones e interfaces *Seguridad e integridad de los datos*	AIS-04.1	¿La arquitectura de seguridad de los datos se ha diseñado conforme a una norma del sector (por ejemplo, CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	La arquitectura de seguridad de los datos de AWS se ha diseñado para incorporar las principales prácticas del sector. Consulte las certificaciones, informes y documentos técnicos de AWS para obtener información adicional sobre las distintas prácticas que sigue AWS (disponibles en http://aws.amazon.com/compliance).
Garantías de auditoría y conformidad *Planificación de auditorías*	AAC-01.1	¿Elabora declaraciones de auditoría con un formato estructurado aceptado por la industria (por ejemplo, CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, el programa de garantías/auditoría de administración de cloud computing de ISACA, etc.)?	AWS obtiene determinadas certificaciones del sector y acreditaciones independientes, además de ofrecer determinadas certificaciones, informes y otra documentación relevante directamente a los clientes de AWS.
Garantías de auditoría y conformidad *Auditorías independientes*	AAC-02.1	¿Permite que los clientes consulten los informes SOC2/ISO 27001 u otros informes de auditoría o certificación independientes?	AWS facilita directamente a nuestros clientes, de conformidad con acuerdos de nivel de servicios, acreditaciones independientes, certificaciones, el informe Service Organization Controls (SOC) y otros informes de conformidad pertinentes. La certificación ISO 27001 de AWS se puede descargar aquí http://do.awsstatic.com/certifications/iso_27001_global_certification.pdf. El informe SOC 3 de AWS se puede descargar aquí: https://do.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf. AWS Security analiza con regularidad todas las direcciones IP de punto de enlace de los servicios expuestas a Internet a fin de detectar vulnerabilidades (estos análisis no incluyen las instancias de los clientes). AWS Security notifica al respecto a las partes correspondientes para remediar todas las vulnerabilidades detectadas. Asimismo, empresas de seguridad independientes realizan con regularidad evaluaciones de amenazas de vulnerabilidades externas. Los resultados y las recomendaciones derivados de estas evaluaciones se clasifican y, además, se entregan a los equipos directivos de AWS.
	AAC-02.2	¿Realiza pruebas de intrusión de red de la infraestructura de servicios en la cloud con regularidad de conformidad con las directrices y las prácticas recomendadas del sector?	
	AAC-02.3	¿Realiza pruebas de intrusion de las aplicaciones de la infraestructura de la cloud con regularidad de conformidad con las directrices y las prácticas recomendadas del sector?	

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
	AAC-02.4	¿Realiza auditorías internas con regularidad de conformidad con las directrices y las prácticas recomendadas del sector?	Asimismo, el entorno de control de AWS está sujeto a varias auditorías internas y externas y evaluaciones de riesgos. AWS colabora con auditores independientes y organismos de certificación externos para revisar y probar el entorno de control global de AWS.
	AAC-02.5	¿Realiza auditorías externas con regularidad de conformidad con las directrices y las prácticas recomendadas del sector?	
	AAC-02.6	¿Los resultados de las pruebas de intrusión se encuentran disponibles cuando las organizaciones los solicitan?	
	AAC-02.7	¿Los resultados de las auditorías internas y externas se encuentran disponibles cuando las organizaciones los solicitan?	
	AAC-02.8	¿Tiene un programa de auditorías internas que permita la auditoría multifuncional de las evaluaciones?	
Garantías de auditoría y conformidad *Asignación normativa de los sistemas de información*	AAC-03.1	¿Tiene la posibilidad de segmentar o cifrar de manera lógica los datos de los clientes, como los datos que puedan producirse para una única organización, sin necesidad de obtener acceso de forma inadvertida a los datos de otras organizaciones?	Todos los datos almacenados por AWS en nombre de los clientes tienen capacidades sólidas de control y seguridad de aislamiento de organizaciones. Los clientes mantienen el control y la titularidad de sus datos, por lo que son responsables de cifrarlos. AWS permite a los clientes utilizar sus propios mecanismos de cifrado prácticamente para todos los servicios, entre otros, S3, EBS, SimpleDB y EC2. Los túneles IPSec con VPC también están cifrados. Asimismo, los clientes pueden usar AWS Key Management Systems (KMS) para crear y controlar las claves de cifrado (consulte https://aws.amazon.com/kms/). Consulte el documento técnico de seguridad de la cloud de AWS para obtener información adicional, que se encuentra disponible en http://aws.amazon.com/security AWS permite a los clientes realizar sus propios backups en cintas con su propio proveedor de servicios de backup en cinta. No obstante, AWS no ofrece el servicio de backup en cinta. Los servicios Amazon S3 y Glacier se han diseñado para abordar la probabilidad de que se produzcan pérdidas de datos con un porcentaje próximo a cero, y la durabilidad equivalente de copias en varios sitios de los objetos de datos se consigue con la redundancia del almacenamiento de los datos. Para obtener información acerca de la redundancia y la durabilidad de los datos, consulte el sitio web de AWS.
	AAC-03.2	¿Tiene la posibilidad de recuperar datos de un cliente concreto en caso de que se produzca un produzca un error o pérdida de datos?	
	AAC-03.3	¿Tiene la posibilidad de restringir el almacenamiento de datos del cliente a países o ubicaciones geográficas específicas?	Los clientes de AWS indican en qué región física se ubicará su contenido. AWS no moverá el contenido de los clientes desde las regiones seleccionadas sin notificárselo, a menos que resulte necesario a efectos de cumplir la legislación o por petición de organismos gubernamentales. En el momento de redactar este documento, hay doce regiones: EE.UU. Este (Norte de Virginia), EE.UU. Oeste (Oregón), EE.UU. Oeste (Norte de California), AWS GovCloud (EE. UU.) (Oregón), UE (Irlanda), UE (Fráncfort), Asia Pacífico (Seúl), Asia Pacífico (Singapur), Asia Pacífico (Tokio), Asia Pacífico (Sídney), China (Beijing) y América del Sur (São Paulo).

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
	AAC-03.4	¿Tiene un programa que incluya la posibilidad de monitorear los cambios en los requisitos normativos en las jurisdicciones pertinentes, adaptar el programa de seguridad a los requisitos legales y garantizar la conformidad con los requisitos normativos pertinentes?	AWS monitorea los requisitos legales y normativos pertinentes. Consulte la norma ISO 27001, anexo 18, para obtener información adicional. Un auditor independiente ha validado y certificado que AWS cumple con el estándar de certificación ISO 27001.
Administración de la continuidad del negocio y capacidad operativa *Planificación de la continuidad del negocio*	BCR-01.1	¿Ofrece a las organizaciones opciones de alojamiento resistentes desde el punto de vista geográfico?	Los centros de datos están agrupados en varias regiones del mundo. AWS ofrece a los clientes la flexibilidad necesaria para colocar las instancias y almacenar datos en varias regiones geográficas, así como en zonas de disponibilidad múltiples dentro de cada región. Los clientes deben planificar el uso que realizan de AWS para poder utilizar varias regiones y zonas de disponibilidad. Consulte el documento técnico de información general sobre la seguridad de la cloud de AWS para obtener información adicional, que se encuentra disponible en http://aws.amazon.com/security.
	BCR-01.2	¿Ofrece a las organizaciones funciones de conmutación por error del servicio de infraestructura a otros proveedores?	
Administración de la continuidad del negocio y capacidad operativa *Pruebas de continuidad del negocio*	BCR-02.1	¿Los planes de continuidad del negocio están sujetos a pruebas a intervalos regulares o a cambios de entorno u organizativos importantes a fin de garantizar una eficacia constante?	Los planes y las políticas de continuidad del negocio de AWS se han desarrollado y probado de conformidad con las normas de la ISO 27001. Consulte la norma ISO 27001, anexo A, dominio 17, para obtener información adicional acerca de AWS y la continuidad del negocio.
Administración de la continuidad del negocio y capacidad operativa *Energía y telecomunicaciones*	BCR-03.1	¿Ofrece a las organizaciones documentación en la que se muestra la ruta que siguen los datos cuando se transfieren entre sus sistemas?	Los clientes de AWS designan en qué región física se ubicarán sus datos y servidores. AWS no moverá el contenido de los clientes desde las regiones seleccionadas sin notificárselo, a menos que resulte necesario a efectos de cumplir la legislación o por petición de organismos gubernamentales. En los informes SOC de AWS se ofrece información adicional. Los clientes también pueden elegir la ruta de acceso de red a las instalaciones de AWS, incluso a través de redes privadas y dedicadas en las que el cliente controla el enrutamiento del tráfico.
	BCR-03.2	¿Pueden las organizaciones definir cómo se transportan los datos y a través de que jurisdicciones legales?	
Administración de la continuidad del negocio y capacidad operativa Documentación	BCR-04.1	¿Se ha puesto la documentación de los sistemas de información (por ejemplo, guías del administrador y del usuario, diagramas de arquitectura, etc.) a disposición del personal autorizado para garantizar la configuración, la instalación y el funcionamiento del sistema de información?	La documentación del sistema de información se pone a disposición del personal de AWS a nivel interno a través de la intranet de Amazon. Consulte el documento técnico de seguridad de la cloud de AWS para obtener información adicional, que se encuentra disponible en http://aws.amazon.com/security/. Consulte la norma ISO 27001, anexo A, dominio 12.
Administración de la continuidad del negocio y capacidad operativa *Riesgos medioambientales*	BCR-05.1	¿Se anticipa y diseña protección física contra daños por desastres o fenómenos naturales y ataques deliberados y, en su caso, se aplican contramedidas?	Los centros de datos de AWS incorporan una protección física frente a riesgos medioambientales. Un auditor independiente ha validado la protección física de AWS frente a riesgos ambientales, que ha certificado su conformidad con las prácticas recomendadas de la norma ISO 27002. Consulte la norma ISO 27001, anexo A, dominio 11.

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
Administración de la continuidad del negocio y capacidad operativa *Ubicación del equipo*	BCR-06.1	¿Está alguno de sus centros de datos ubicado en un lugar con alta probabilidad o incidencia de riesgos medioambientales de gran impacto (como inundaciones, tornados, terremotos, huracanes, etc.)?	Los centros de datos de AWS incorporan una protección física frente a riesgos medioambientales. Un auditor independiente ha validado la protección física de AWS frente a riesgos ambientales, que ha certificado su conformidad con las prácticas recomendadas de la norma ISO 27002. Consulte la norma ISO 27001, anexo A, dominio 11.
Administración de la continuidad del negocio y capacidad operativa *Mantenimiento del equipo*	BCR-07.1	En caso de que se utilice una infraestructura virtual, ¿su solución en la cloud incluye funciones de recuperación y restablecimiento independientes para el hardware?	La funcionalidad de snapshots de EBS permite a los clientes capturar y restablecer imágenes de máquinas virtuales en cualquier momento. Los clientes pueden exportar sus AMI y utilizarlas en las instalaciones o con otro proveedor (sujetos a restricciones de licencias de software). Consulte el documento técnico de seguridad de la cloud de AWS para obtener información adicional, que se encuentra disponible en http://aws.amazon.com/security.
	BCR-07.2	Si se usa infraestructura virtual, ¿proporciona a las organizaciones la capacidad de restaurar una máquina virtual a un estado anterior en el tiempo?	
	BCR-07.3	Si se usa infraestructura virtual, ¿permite descargar y migrar las imágenes de máquina virtual a un nuevo proveedor de servicios en la cloud?	
	BCR-07.4	Si se usa infraestructura virtual, ¿están disponibles las imágenes de la máquina para el cliente de forma que pueda replicar esas imágenes en su propia ubicación de almacenamiento fuera de las instalaciones?	
	BCR-07.5	¿Su solución en la cloud incluye funciones de restauración y recuperación independientes del software o proveedor?	
Administración de la continuidad del negocio y capacidad operativa *Errores de alimentación del equipo*	BCR-08.1	¿Se aplican redundancias y mecanismos de seguridad para proteger los equipos frente a interrupciones de servicios públicos (por ejemplo, cortes de alimentación, interrupciones de red, etc.)?	El equipo de AWS está protegido frente a interrupciones de los servicios públicos de conformidad con la norma ISO 27001. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001. En los informes SOC de AWS se ofrece información adicional acerca de los controles disponibles para minimizar el efecto del funcionamiento inadecuado o el desastre físico en el equipo y en las instalaciones del centro de datos. Asimismo, consulte el documento técnico de seguridad en la cloud de AWS, disponible en http://aws.amazon.com/security.

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
Administración de la continuidad del negocio y capacidad operativa *Análisis del impacto*	BCR-09.1	¿Ofrece a las organizaciones informes y visibilidad constantes sobre el desempeño del acuerdo de nivel de servicios (SLA) operativo?	AWS CloudWatch proporciona la monitorización de los recursos de la cloud de AWS y de las aplicaciones que los clientes ejecutan en AWS. Consulte aws.amazon.com/cloudwatch para obtener información adicional. AWS también publica la información actualizada sobre la disponibilidad del servicio en el Panel de estado del servicio. Visite status.aws.amazon.com.
	BCR-09.2	¿Pone a disposición de las organizaciones métricas de seguridad de la información basadas en estándares (CSA, CAMM, etc.)?	
	BCR-09.3	¿Ofrece a los clientes informes y visibilidad constantes acerca del desempeño de su acuerdo de nivel de servicios?	
Administración de la continuidad del negocio y capacidad operativa *Política*	BCR-10.1	¿Se han establecido políticas y procedimientos y, en su caso, están disponibles para que todo el personal desempeñe correctamente las funciones relacionadas con las operaciones de los servicios?	Se han establecido políticas y procedimientos a través del marco de seguridad de la información de AWS basados en el estándar NIST 800-53, ISO 27001, ISO 27017, ISO 27018 e ISO 9001 y las disposiciones de PCI DSS. Consulte el documento técnico sobre riesgos y conformidad de AWS para obtener información adicional, que se encuentra disponible en http://aws.amazon.com/compliance.
Administración de la continuidad del negocio y capacidad operativa *Política de retención*	BCR-11.1	¿Ofrece opciones de control técnico para exigir el cumplimiento de las políticas de retención de datos de la organización?	AWS ofrece a los clientes la posibilidad de eliminar sus datos. No obstante, los clientes de AWS mantienen el control y la titularidad de los datos, por lo que tienen la responsabilidad de administrar la retención de los datos en función de sus propias necesidades. Consulte el documento técnico de seguridad de la cloud de AWS para obtener información adicional, que se encuentra disponible en http://aws.amazon.com/security. AWS ofrece un alto nivel de protección de la privacidad de los clientes, por lo que está alerta a la hora de determinar qué requisitos de conformidad con las leyes debemos cumplir. AWS no duda en impugnar las órdenes de las autoridades si considera que carecen de fundamentos sólidos. Para obtener información adicional, consulte https://aws.amazon.com/compliance/data-privacy-faq/.
	BCR-11.2	¿Dispone de un procedimiento documentado para responder a las solicitudes que los gobiernos o terceros realizan de los datos de las organizaciones?	
	BCR-11.4	¿Dispone de mecanismos de backup o redundancia para garantizar la conformidad con los requisitos legales, normativos, contractuales o del negocio?	Los mecanismos de backup y redundancia de AWS se han desarrollado y probado de conformidad con las normas de la ISO 27001. Consulte la norma ISO 27001, anexo A, dominio 12, y el informe SOC 2 de AWS para obtener información adicional sobre los mecanismos de backup y redundancia de AWS.
	BCR-11.5	¿Prueba sus mecanismos de backup y redundancia al menos una vez al año?	
Administración de control de cambios y configuración *Nuevo desarrollo / adquisición*	CCC-01.1	¿Se han establecido políticas y procedimientos de autorización de la administración para desarrollar o adquirir nuevas aplicaciones, sistemas, bases de datos, infraestructuras, servicios, operaciones e instalaciones?	Se han establecido políticas y procedimientos a través del marco de seguridad de la información de AWS basados en el estándar NIST 800-53, ISO 27001, ISO 27017, ISO 27018 e ISO 9001 y las disposiciones de PCI DSS. Los usuarios con y sin experiencia en AWS pueden encontrar información útil sobre los servicios, que abarca tanto introducciones como descripciones de características avanzadas, en la sección de documentación de AWS de nuestro sitio web en https://aws.amazon.com/documentation/.
	CCC-01.2	¿Hay disponible documentación que describa la instalación, configuración y uso de los productos, servicios o características?	

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
Administración de control de cambios y configuración *Desarrollo subcontratado*	CCC-02.1	¿Cuenta con controles para garantizar el cumplimiento de las normas de calidad en todos los desarrollos de software?	AWS no suele externalizar el desarrollo de software. AWS incorpora normas de calidad como parte de los procesos del ciclo de vida de desarrollo del sistema (SDLC). Consulte la norma ISO 27001, anexo A, dominio 14, para obtener información adicional. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
	CCC-02.2	¿Dispone de controles para detectar defectos de seguridad del código fuente en las actividades de desarrollo de software externalizadas?	
Administración de control de cambios y configuración *Pruebas de calidad de la administración*	CCC-03.1	¿Ofrece a las organizaciones documentación en la que se describa el proceso de control de calidad?	AWS mantiene una certificación ISO 9001. Se trata de una validación independiente del sistema de calidad de AWS que determina que las actividades de AWS cumplen los requisitos de la norma ISO 9001. Para informar a los clientes de los eventos de seguridad y privacidad se utilizan los boletines de seguridad de AWS. Los clientes pueden suscribirse a la fuente RSS de boletines de seguridad de AWS en nuestro sitio web. Consulte aws.amazon.com/security/security-bulletins/. AWS también publica la información actualizada sobre la disponibilidad del servicio en el Panel de estado del servicio. Visite status.aws.amazon.com. El ciclo de vida de desarrollo de sistemas (SDLC) de AWS incorpora las prácticas recomendadas del sector, que incluyen las revisiones formales de diseño de AWS Security Team, el modelado de amenazas y la realización de una evaluación de riesgos. Consulte el documento técnico de información general sobre los procesos de seguridad de AWS para obtener información adicional. Además, consulte la norma ISO 27001, anexo A, dominio 14 para obtener más información. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
	CCC-03.2	¿Hay disponible documentación en la que se describan los problemas conocidos con determinados productos o servicios?	
	CCC-03.3	¿Existen políticas y procedimientos para clasificar y remediar los errores registrados y las vulnerabilidades de seguridad de los productos y servicios?	
	CCC-03.4	¿Existen mecanismos para garantizar que todos los elementos de código de depuración y pruebas se han eliminado de las versiones de software publicadas?	
Administración de control de cambios y configuración *Instalaciones de software no autorizadas*	CCC-04.1	¿Dispone de controles para restringir y monitorear la instalación de software no autorizado en los sistemas?	El programa, los procesos y los procedimientos de AWS para administrar software malicioso están en consonancia con las normas de la ISO 27001. Consulte la norma ISO 27001, anexo A, dominio 12, para obtener información adicional. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
Administración de control de cambios y configuración *Cambios en producción*	CCC-05.1	¿Ofrece a las organizaciones documentación en la que se describan los procedimientos de administración de los cambios en producción y sus funciones, derechos y responsabilidades en este sentido?	En los informes SOC de AWS, se ofrece información general acerca de los controles existentes para administrar los cambios en el entorno de AWS. Además, consulte la norma ISO 27001, anexo A, dominio 12, para obtener información adicional. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
Seguridad de los datos y administración del ciclo de vida de la información *Clasificación*	DSI-01.1	¿Proporciona alguna capacidad para identificar las máquinas virtuales mediante etiquetas de política/metadatos (por ejemplo, las etiquetas se pueden utilizar para evitar que los sistemas operativos invitados realicen las acciones de arrancar, crear instancias y transportar datos en el país incorrecto, entre otras acciones)?	Las máquinas virtuales se asignan a los clientes como parte del servicio de EC2. Los clientes mantienen el control de los recursos que se utilizan y dónde estos residen. Consulte el sitio web de AWS http://aws.amazon.com para obtener información adicional.
	DSI-01.2	¿Ofrece la posibilidad de identificar hardware a través de etiquetas de hardware/metadatos/de políticas (por ejemplo, TXT/TPM, VN- Tag, etc.)?	AWS ofrece la posibilidad de etiquetar los recursos de EC2. Las etiquetas de EC2, un tipo de metadatos, se pueden utilizar para crear nombres sencillos, mejorar la capacidad de búsqueda y mejorar la coordinación entre varios usuarios. La consola de administración de AWS también admite el etiquetado.
	DSI-01.3	¿Tiene la posibilidad de utilizar la ubicación geográfica del sistema como un factor de autenticación?	AWS ofrece la opción del acceso de usuario condicional en función de la dirección IP. Los clientes pueden agregar condiciones para controlar la forma en que sus usuarios pueden utilizar AWS (por ejemplo, la hora del día, la dirección IP de origen, o en función de si utilizan o no SSL).
	DSI-01.4	¿Puede proporcionar la ubicación física y geográfica del almacenamiento de los datos de un inquilino bajo petición?	AWS ofrece a los clientes la flexibilidad necesaria para colocar instancias y almacenar datos en varias regiones geográficas. Los clientes de AWS designan en qué región física se ubicarán sus datos y servidores. AWS no moverá el contenido de los clientes desde las regiones seleccionadas sin notificárselo, a menos que resulte necesario a efectos de cumplir la legislación o por petición de organismos gubernamentales. En el momento de redactar este documento hay doce regiones: EE.UU. Este (Norte de Virginia), EE.UU. Oeste (Oregón), EE.UU. Oeste (Norte de California), AWS GovCloud (EE.UU.) (Oregón), UE (Irlanda), UE (Fráncfort), Asia Pacífico (Seúl), Asia Pacífico (Singapur), Asia Pacífico (Tokio), Asia Pacífico (Sídney), China (Pekín) y América del Sur (São Paulo).
	DSI-01.5	¿Puede proporcionar la ubicación física y geográfica del almacenamiento de los datos de un inquilino con anticipación?	
	DSI-01.6	¿Sigue un estándar de etiquetado estructurado de los datos (por ejemplo, ISO 15489, la especificación del catálogo XML de Oasis, las directrices sobre el tipo de datos de CSA)?	Los clientes de AWS mantienen el control y la titularidad de sus datos y pueden aplicar un estándar de etiquetado de datos estructurado para satisfacer sus necesidades.
	DSI-01.7	¿Permite que los inquilinos definan ubicaciones geográficas aceptables para el direccionamiento de los datos o la creación de instancias de los recursos?	AWS ofrece a los clientes la flexibilidad necesaria para colocar instancias y almacenar datos en varias regiones geográficas. Los clientes de AWS designan en qué región física se ubicarán sus datos y servidores. AWS no moverá el contenido de los clientes desde las regiones seleccionadas sin notificárselo, a menos que resulte necesario a efectos de cumplir la legislación o por petición de organismos gubernamentales. En el momento de redactar este documento hay doce regiones: EE.UU. Este (Norte de Virginia), EE.UU. Oeste (Oregón), EE.UU. Oeste (Norte de California), AWS GovCloud (EE.UU.) (Oregón), UE (Irlanda), UE (Fráncfort), Asia Pacífico (Seúl), Asia Pacífico (Singapur), Asia Pacífico (Tokio), Asia Pacífico (Sídney), China (Pekín) y América del Sur (São Paulo).
Seguridad de los datos y administración del ciclo de vida de la información *Flujos/Inventarios de datos*	DSI-02.1	¿Realiza inventarios de los flujos de datos, los documenta y los mantiene en el caso de los datos que residen (permanente o temporalmente) dentro de las aplicaciones de los servicios y los sistemas y redes de la infraestructura?	Los clientes de AWS indican en qué región física se ubicará su contenido. AWS no moverá el contenido de los clientes desde las regiones seleccionadas sin notificárselo, a menos que resulte necesario a efectos de cumplir la legislación o por petición de organismos gubernamentales. En el momento de redactar este documento hay doce regiones: EE.UU. Este (Norte de Virginia), EE.UU. Oeste (Oregón), EE.UU. Oeste (Norte de California), AWS GovCloud (EE.UU.) (Oregón), UE (Irlanda), UE (Fráncfort), Asia Pacífico (Seúl), Asia Pacífico (Singapur), Asia Pacífico (Tokio), Asia Pacífico (Sídney), China (Pekín) y América del Sur (São Paulo).

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
	DSI-02.2	¿Puede garantizar que la migración de datos no se realice más allá del área geográfica definida?	
Seguridad de los datos y administración del ciclo de vida de la información *Transacciones de eCommerce*	DSI-03.1	¿Proporciona a los inquilinos metodologías abiertas de cifrado (3.4ES, AES, etc.) para que protejan sus datos si es necesario desplazarse por las redes públicas (p. ej., Internet)?	Todas las API de AWS se encuentran disponibles a través de puntos finales protegidos por Secure Shell (SSH, shell seguro) que ofrecen autenticación del servidor. AWS permite a los clientes utilizar sus propios mecanismos de cifrado prácticamente para todos los servicios, entre otros, S3, EBS, SimpleDB y EC2. Los túneles IPSec con VPC también están cifrados. Asimismo, los clientes pueden usar AWS Key Management Systems (KMS) para crear y controlar las claves de cifrado (consulte https://aws.amazon.com/kms/). Además, los clientes también pueden utilizar tecnologías de cifrado de terceros. Consulte el documento técnico de seguridad de la cloud de AWS para obtener información adicional, que se encuentra disponible en http://aws.amazon.com/security.
	DSI-03.2	¿Utiliza metodologías de cifrado abierto siempre que los componentes de la infraestructura necesitan comunicarse entre sí a través de redes públicas (por ejemplo, la replicación de los datos de un entorno a otro a través de Internet)?	
Seguridad de los datos y administración del ciclo de vida de la información *Política de administración, etiquetado y seguridad*	DSI-04.1	¿Existen políticas y procedimientos para el etiquetado, la gestión y la seguridad de los datos y de los objetos que contienen datos?	Los clientes de AWS mantienen el control y la titularidad de los datos y pueden aplicar procedimientos y una política de etiquetado y administración para satisfacer sus necesidades.
	DSI-04.2	¿Se utilizan mecanismos para etiquetar recursos heredados para objetos que actúan como contenedores agregados de los datos?	
Seguridad de los datos y administración del ciclo de vida de la información *Datos no relacionados con la producción*	DSI-05.1	¿Dispone de procedimientos para garantizar que los datos de producción no se repliquen ni utilicen en entornos no productivos?	Los clientes de AWS preservan el control y la titularidad de sus propios datos. AWS les ofrece a los clientes la posibilidad de mantener y desarrollar entornos productivos y no productivos. Es responsabilidad del cliente garantizar que los datos de producción no se repliquen en entornos no productivos.
Seguridad de los datos y administración del ciclo de vida de la información *Titularidad/ Custodia*	DSI-06.1	¿Las responsabilidades sobre la custodia de datos se definieron, asignaron, documentaron y comunicaron?	Los clientes de AWS preservan el control y la titularidad de sus propios datos. Consulte el Acuerdo de Cliente de AWS para obtener más información.

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
Seguridad de los datos y administración del ciclo de vida de la información *Eliminación segura*	DSI-07.1	¿Admite la eliminación segura (por ejemplo, desmagnetización/borrado criptográfico) de los datos archivados y respaldados según lo determine el inquilino?	Cuando un dispositivo de almacenamiento alcanza el final de su vida útil, los procedimientos de AWS incluyen un proceso de retirada diseñado para prevenir que los datos de los clientes queden expuestos al acceso de personas no autorizadas. AWS utiliza las técnicas detalladas en DoD 5220.22-M ("Manual de operaciones del programa de seguridad industrial nacional") o NIST 800-88 ("Directrices para el saneamiento de soportes") para destruir datos como parte del proceso de retirada. En caso de que no se pueda retirar un dispositivo de hardware con estos procedimientos, el dispositivo se desmagnetizará o destruirá físicamente de conformidad con las prácticas estándar del sector. Consulte el documento técnico de seguridad de la cloud de AWS para obtener información adicional, que se encuentra disponible en http://aws.amazon.com/security. Los volúmenes de Amazon EBS se presentan como dispositivos de bloques sin formato y sin procesar que se borran antes de que puedan utilizarse. El borrado se realiza inmediatamente antes de su reutilización, de modo que pueda asegurarse de que el proceso de borrado se complete con éxito. Si usted tiene procedimientos que requieren que todos los datos se borren con un método específico, como los que se detallan en DoD 5220.22-M ("Manual de operaciones del programa de seguridad industrial nacional ") o NIST 800-88 ("Directrices para el saneamiento de soportes"), cuenta con la opción de hacerlo en Amazon EBS. Debe realizar un procedimiento de borrado especializado antes de eliminar el volumen, con el fin de cumplir con los requisitos que estableció. El cifrado de datos confidenciales, por lo general, es una buena práctica de seguridad, y AWS proporciona la capacidad de cifrar volúmenes EBS y sus instantáneas con AES-256. El cifrado se realiza en los servidores que alojan las instancias de EC2, por lo que los datos se cifran a medida que estos circulan entre las instancias de EC2 y el almacenamiento de EBS. Para poder hacer esto eficazmente y con baja latencia, la característica de cifrado de EBS solo está disponible en los tipos de instancias más potentes de EC2 (como M3, C3, R3, G2).
	DSI-07.2	¿Puede ofrecer un procedimiento público para cerrar la prestación del servicio, incluida la garantía de sanear todos los recursos informáticos de los datos del inquilino cuando un cliente ha cerrado su entorno o ha anulado un recurso?	
Seguridad del centro de datos *Administración de recursos*	DCS-01.1	¿Conserva un inventario completo de todos los recursos de vital importancia en el que conste la titularidad del recurso?	De conformidad con el estándar ISO 27001, a los recursos de hardware de AWS se les asigna un propietario, de cuyo seguimiento y monitoreo se encarga el personal de AWS con herramientas de administración del inventario propietarias de AWS. El equipo de la cadena de suministro y contratación de AWS mantiene relaciones con todos los proveedores de AWS. Consulte la norma ISO 27001; anexo A, dominio 8, para obtener información adicional. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
	DCS-01.2	¿Conserva un inventario completo de todas las relaciones con proveedores de vital importancia?	
Seguridad del centro de datos *Puntos de acceso controlados*	DCS-02.1	¿Se implementaron perímetros de seguridad física (por ejemplo, vallas, muros, barreras, guardias, portones, vigilancia electrónica, mecanismos de autenticación física, recepción y patrullas de seguridad)?	Los controles de seguridad física incluyen, pero no se limitan a, controles perimetrales como vallas, muros, personal de seguridad, videovigilancia, sistemas de detección de intrusiones y otros medios electrónicos. En los informes SOC de AWS, se ofrecen detalles adicionales acerca de las actividades de control específicas que ejecuta AWS. Consulte la norma ISO 27001; anexo A, dominio 11, para obtener información adicional. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
Seguridad del centro de datos *Identificación de equipos*	DCS-03.1	¿La identificación automática del equipo se utiliza como un método para validar la integridad de la autenticación en función de una ubicación conocida del equipo?	AWS administra la identificación de equipos de conformidad con el estándar ISO 27001. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
Seguridad del centro de datos *Autorización externa*	DCS-04.1	¿Ofrece a los inquilinos documentación en la que se describan los escenarios en que los datos se pueden mover de una ubicación física a otra (por ejemplo, copias de seguridad remotas, conmutaciones por error para la continuidad empresarial y replicación)?	Los clientes pueden designar en qué región física se ubicarán sus datos. AWS no moverá el contenido de los clientes desde las regiones seleccionadas sin notificárselo, a menos que resulte necesario a efectos de cumplir la legislación o por petición de organismos gubernamentales. Consulte el documento técnico de seguridad de la cloud de AWS para obtener información adicional, que se encuentra disponible en http://aws.amazon.com/security.
Seguridad del centro de datos *Equipos externos*	DCS-05.1	¿Ofrece a los inquilinos documentación en la que se describen las políticas y los procedimientos que rigen la administración de recursos y la incorporación de equipos?	De conformidad con el estándar ISO 27001, cuando un dispositivo de almacenamiento alcanza el final de su vida útil, los procedimientos de AWS incluyen un proceso de retirada diseñado para prevenir que los datos de los clientes queden expuestos al acceso de personas no autorizadas. AWS utiliza las técnicas detalladas en DoD 5220.22-M ("Manual de operaciones del programa de seguridad industrial nacional") o NIST 800-88 ("Directrices para el saneamiento de soportes") para destruir datos como parte del proceso de retirada. En caso de que no se pueda retirar un dispositivo de hardware con estos procedimientos, el dispositivo se desmagnetizará o destruirá físicamente de conformidad con las prácticas estándar del sector. Consulte la norma ISO 27001; anexo A, dominio 8, para obtener información adicional. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
Seguridad del centro de datos *Política*	DCS-06.1	¿Puede demostrar que se han establecido las políticas, los estándares y los procedimientos para mantener un entorno de trabajo seguro y protegido en oficinas, salas, instalaciones y espacios seguros?	AWS colabora con organismos de certificación externos y auditores independientes para revisar y validar el cumplimiento de las estructuras de conformidad. En los informes SOC de AWS, se ofrecen detalles adicionales acerca de las actividades específicas de control de la seguridad física que ejecuta AWS. Consulte la norma ISO 27001; anexo A, dominio 11, para obtener información adicional. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
	DCS-06.2	¿Puede demostrar que su personal y los terceros involucrados fueron capacitados sobre sus políticas, estándares y procedimientos documentados?	De conformidad con el estándar ISO 27001, todos los empleados de AWS realizan una capacitación periódica sobre seguridad de la información que requiere un reconocimiento para completarla. Las auditorías de conformidad se realizan periódicamente a fin de validar que los empleados puedan conocer y seguir las políticas establecidas. Consulte el documento técnico de seguridad de la cloud de AWS para obtener más información, que se encuentra disponible en http://aws.amazon.com/security. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple el estándar de certificación ISO 27001. Además, en los informes SOC 1 y SOC 2 puede encontrar información adicional.
Seguridad del centro de datos *Autorización de espacio seguro*	DCS-07.1	¿Permite que los inquilinos especifiquen en qué ubicaciones geográficas pueden entrar y salir los datos (para abordar las consideraciones sobre la jurisdicción en función de dónde están almacenados los datos y desde dónde se accede a ellos)?	Los clientes de AWS pueden designar en qué región física se ubicarán sus datos. AWS no moverá el contenido de los clientes desde las regiones seleccionadas sin notificárselo, a menos que resulte necesario a efectos de cumplir la legislación o por petición de organismos gubernamentales. En el momento de redactar este documento hay doce regiones: EE.UU. Este (Norte de Virginia), EE.UU. Oeste (Oregón), EE.UU. Oeste (Norte de California), AWS GovCloud (EE.UU.) (Oregón), UE (Irlanda), UE (Fráncfort), Asia Pacífico (Seúl), Asia Pacífico (Singapur), Asia Pacífico (Tokio), Asia Pacífico (Sídney), China (Pekín) y América del Sur (São Paulo).

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
Seguridad del centro de datos *Entrada de personas no autorizadas*	DCS-08.1	¿Los puntos de entrada y salida, como las áreas de servicio y otros puntos donde personal no autorizado puede entrar en las instalaciones, están supervisados, controlados y aislados del procesamiento y almacenamiento de los datos?	El acceso físico está estrictamente controlado en el perímetro y en los puntos de acceso del edificio e incluye, entre otros aspectos, personal de seguridad profesional mediante videovigilancia, sistema de detección de intrusiones y otros recursos electrónicos. El personal autorizado debe confirmar una autenticación de dos factores como mínimo dos veces para acceder a los pisos del centro de datos. Los puntos de acceso físico a las ubicaciones de los servidores se graban con cámaras de televisión de circuito cerrado (closed circuit television camera, CCTV), tal y como se define en la política de seguridad física del centro de datos de AWS. Los auditores independientes externos revisan los mecanismos de seguridad física de AWS durante las auditorías de nuestra conformidad con SOC, PCI DSS, ISO 27001 y FedRAMP.
Seguridad del centro de datos *Acceso de los usuarios*	DCS-09.1	¿Restringe el acceso físico a las funciones y los recursos de información de parte de los usuarios y el personal de soporte?	
Administración de claves de cifrado *Concesión de derechos*	EKM-01.1	¿Cuenta con políticas de administración de claves que vinculen las claves con los propietarios identificables?	AWS les ofrece a los clientes la posibilidad de utilizar su propio mecanismo de cifrado prácticamente para todos los servicios, incluidos S3, EBS y EC2. También se cifran las sesiones de VPC. Asimismo, los clientes pueden usar AWS Key Management Systems (KMS) para crear y controlar las claves de cifrado (consulte https://aws.amazon.com/kms/). Internamente, AWS establece y administra claves de cifrado para la criptografía necesaria empleada en la infraestructura de AWS. Se utiliza un gestor de credenciales y claves seguras desarrollado por AWS para crear, proteger y distribuir claves simétricas, así como para proteger y distribuir credenciales de AWS necesarias en los hosts, claves públicas y privadas de RSA y certificaciones X.509. Los auditores independientes externos revisan los procesos de cifrado de AWS como parte de nuestro programa continuado de conformidad con SOC, PCI DSS, ISO 27001 y FedRAMP.
Administración de claves de cifrado *Generación de claves*	EKM-02.1	¿Tiene la posibilidad de admitir la creación de claves de cifrado exclusivas para cada inquilino?	AWS permite a los clientes utilizar sus propios mecanismos de cifrado prácticamente para todos los servicios, entre otros, S3, EBS y EC2. Los túneles IPSec con VPC también están cifrados. Asimismo, los clientes pueden usar AWS Key Management Systems (KMS) para crear y controlar las claves de cifrado (consulte https://aws.amazon.com/kms/). Consulte los informes SOC de AWS para obtener más información sobre KMS. Además, consulte el documento técnico de seguridad de la cloud de AWS para obtener información adicional, que se encuentra disponible en http://aws.amazon.com/security. Internamente, AWS establece y administra claves de cifrado para la criptografía necesaria empleada en la infraestructura de AWS. AWS produce, controla y distribuye claves criptográficas simétricas mediante los procesos y la tecnología de administración de claves del sistema de información de AWS aprobados por el NIST. Se utiliza un gestor de credenciales y claves seguras desarrollado por AWS para crear, proteger y distribuir claves simétricas, así como para proteger y distribuir credenciales de AWS necesarias en los hosts, claves públicas y privadas de RSA y certificaciones X.509. Los auditores independientes externos revisan los procesos de cifrado de AWS como parte de nuestro programa continuado de conformidad con SOC, PCI DSS, ISO 27001 y FedRAMP.
	EKM-02.2	¿Puede administrar las claves de cifrado en nombre de los inquilinos?	
	EKM-02.3	¿Realiza el mantenimiento de procedimientos de administración de claves?	
	EKM-02.4	¿Ha documentado la titularidad de cada etapa del ciclo de vida de las claves de cifrado?	
	EKM-02.5	¿Utiliza marcos de trabajo de terceros/de código abierto/propios para administrar las claves de cifrado?	

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
Administración de claves de cifrado *Cifrado*	EKM-03.1	¿Cifra los datos inactivos (en disco o almacenados) de los inquilinos dentro del entorno?	AWS permite a los clientes utilizar sus propios mecanismos de cifrado prácticamente para todos los servicios, entre otros, S3, EBS y EC2. Los túneles IPSec con VPC también están cifrados. Asimismo, los clientes pueden usar AWS Key Management Systems (KMS) para crear y controlar las claves de cifrado (consulte https://aws.amazon.com/kms/). Consulte los informes SOC de AWS para obtener más información sobre KMS. Además, consulte el documento técnico de seguridad de la cloud de AWS para obtener información adicional, que se encuentra disponible en http://aws.amazon.com/security.
	EKM-03.2	¿Utiliza el cifrado para proteger los datos y las imágenes de máquina virtual durante la transferencia entre redes e instancias del hipervisor?	
	EKM-03.3	¿Permite las claves de cifrado generadas por los inquilinos o que los inquilinos cifren los datos con una identidad sin acceder a un certificado de clave pública (por ejemplo, el cifrado basado en identidades)?	
	EKM-03.4	¿Cuenta con documentación en la que se establezcan y se definan sus políticas, procedimientos y directrices de administración del cifrado?	
Administración de claves de cifrado *Almacenamiento y acceso*	EKM-04.1	¿Cuenta con un cifrado apropiado para los datos y las plataformas en el que se usen formatos abiertos/validados y algoritmos estándares?	AWS permite a los clientes utilizar sus propios mecanismos de cifrado prácticamente para todos los servicios, entre otros, S3, EBS y EC2. Asimismo, los clientes pueden usar AWS Key Management Systems (KMS) para crear y controlar las claves de cifrado (consulte https://aws.amazon.com/kms/). Consulte los informes SOC de AWS para obtener más información sobre KMS. AWS establece y administra claves de cifrado para la criptografía necesaria empleada en la infraestructura de AWS. AWS produce, controla y distribuye claves criptográficas simétricas mediante los procesos y la tecnología de administración de claves del sistema de información de AWS aprobados por el NIST. Se utiliza un gestor de credenciales y claves seguras desarrollado por AWS para crear, proteger y distribuir claves simétricas, así como para proteger y distribuir credenciales de AWS necesarias en los hosts, claves públicas y privadas de RSA y certificaciones X.509. Los auditores independientes externos revisan los procesos de cifrado de AWS como parte de nuestro programa continuado de conformidad con SOC, PCI DSS, ISO 27001 y FedRAMP.
	EKM-04.2	¿Sus claves de cifrado son mantenidas por el usuario de la cloud o un proveedor de servicios de administración de claves?	
	EKM-04.3	¿Almacena claves de cifrado en la cloud?	
	EKM-04.4	¿Cuenta con tareas de uso y de administración de claves por separado?	
Gobernanza y administración de riesgos *Requisitos de referencia*	GRM-01.1	¿Cuenta con líneas de base documentadas acerca de la seguridad de la información para cada componente de la infraestructura (por ejemplo, hipervisores, sistemas operativos, enrutadores, servidores DNS, etc.)?	De conformidad con el estándar ISO 27001, AWS mantiene líneas de base del sistema para componentes de vital importancia. Consulte la norma ISO 27001; anexo A, dominios 14 y 18, para obtener información adicional. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001. Los clientes pueden proporcionar su propia imagen de máquina virtual. VM Import permite a los clientes importar fácilmente imágenes de máquinas virtuales desde el entorno del cliente a instancias de Amazon EC2.
	GRM-01.2	¿Tiene la posibilidad de controlar constantemente la conformidad de la infraestructura con respecto a las líneas de base de seguridad de la información, así como de hacer informes al respecto?	
	GRM-01.3	¿Permite que los clientes ofrezcan su propia imagen de máquina virtual de confianza para garantizar la conformidad con sus propios estándares internos?	

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
Gobernanza y administración de riesgos *Evaluaciones de riesgos*	GRM-02.1	¿Ofrece datos sobre el estado del control de seguridad a fin de permitir que los inquilinos realicen un monitoreo constante de los estándares del sector (que permita la validación constante por parte del inquilino del estado de control físico y lógico)?	AWS publica certificaciones e informes de auditores independientes a fin de ofrecer a los clientes información considerable acerca de las políticas, los procesos y los controles establecidos y ejecutados por AWS. Se pueden facilitar las certificaciones y los informes correspondientes a los clientes de AWS. Los clientes pueden monitorear constantemente los controles lógicos en sus propios sistemas.
	GRM-02.2	¿Realiza evaluaciones de riesgos relacionadas con los requisitos de gobernanza de datos al menos una vez al año?	De conformidad con el estándar ISO 27001, AWS cuenta con un programa de administración de riesgos para mitigar y administrar los riesgos. Además, AWS cuenta con la certificación ISO 27018. El cumplimiento del estándar ISO 27018 demuestra a los clientes que AWS cuenta con un sistema de controles cuyo objetivo específico es la protección de la privacidad de su contenido. Para obtener más información, consulte las Preguntas Frecuentes sobre el cumplimiento del estándar ISO 27018 en http://aws.amazon.com/compliance/iso-27018-faqs/.
Gobernanza y administración de riesgos *Supervisión de la administración*	GRM-03.1	¿Los directores ejecutivos, comerciales y técnicos son los responsables de mantener la concienciación y el cumplimiento de las políticas, los procedimientos y los estándares de seguridad tanto de su parte como de parte de los empleados relacionados con el área de responsabilidad del director y los empleados?	El entorno de control en Amazon parte del estrato más alto de la empresa. Los altos cargos desempeñan funciones importantes a la hora de definir los valores principales y el tono de la compañía. A todos los empleados se les proporciona el código de conducta y ética empresarial de la compañía y, además, realizan un proceso de capacitación periódica. Las auditorías de conformidad se realizan a fin de que los empleados puedan conocer y seguir las políticas establecidas. Consulte el documento técnico sobre riesgos y conformidad de AWS para obtener información adicional, que se encuentra disponible en http://aws.amazon.com/compliance.
Gobernanza y administración de riesgos *Programa de administración*	GRM-04.1	¿Ofrece a los inquilinos documentación en la que se describa el Information Security Management Program (ISMP, Programa de Administración de la Seguridad de la Información)?	AWS ofrece a nuestros clientes la certificación del estándar ISO 27001. La certificación del estándar ISO 27001 se centra, específicamente, en el ISMS de AWS y mide de qué modo los procesos internos de AWS cumplen con el estándar ISO. El término certificación hace referencia a que un auditor externo independiente acreditado realizó una evaluación de nuestros procesos y controles y confirma que cumplen con los estándares de certificación del estándar ISO 27001. Para obtener más información, consulte el sitio web de preguntas frecuentes sobre el cumplimiento de AWS del estándar ISO 27001 en http://aws.amazon.com/compliance/iso-27001- faqs/.
	GRM-04.2	¿Revisa su Programa de Administración de la Seguridad de la Información (ISMP) al menos una vez al año?	
Gobernanza y administración de riesgos *Respaldo/ Participación de la dirección*	GRM-05.1	¿Garantiza que los proveedores cumplen con las políticas de privacidad y seguridad de la información?	AWS ha establecido un marco y políticas de seguridad de la información en los que se ha integrado el marco certificable ISO 27001 basándose en los controles de ISO 27002, los Principios de los Servicios de Confianza del American Institute of Certified Public Accountants (AICPA), el PCI DSS v3.1 y la Publicación 800-53 del National Institute of Standards and Technology (NIST, Instituto Nacional de Estándares y Tecnología) (Recommended Security Controls for Federal Information Systems). AWS administra las relaciones con terceros de conformidad con el estándar ISO 27001. Los auditores independientes externos revisan los requisitos de los proveedores externos de AWS durante las auditorías de nuestra conformidad con PCI DSS, ISO 27001 y FedRAMP.
Gobernanza y administración de riesgos *Política*	GRM-06.1	¿Las políticas de privacidad y seguridad de la información cumplen con los estándares del sector (ISO-27001, ISO-22307, CoBIT, etc.)?	

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
	GRM-06.2	¿Dispone de acuerdos que garanticen que los proveedores cumplen con las políticas de privacidad y seguridad de la información?	La información sobre los programas de cumplimiento de AWS se encuentra publicada en nuestro sitio web, en http://aws.amazon.com/compliance/.
	GRM-06.3	¿Puede demostrar la debida diligencia en la asignación de los controles, la arquitectura y los procesos a los reglamentos o los estándares?	
	GRM-06.4	¿Divulga información sobre los controles, estándares, certificaciones o reglamentos con los que cumple?	
Gobernanza y administración de riesgos *Cumplimiento de las políticas*	GRM-07.1	¿Se aplica alguna política oficial de carácter disciplinario o de sanciones para los empleados que infringen los procedimientos o las políticas de seguridad?	AWS ofrece políticas de seguridad y capacitación sobre seguridad a los empleados a fin de educarlos con respecto a su función y sus responsabilidades en el ámbito de la seguridad de la información. Los empleados que infrinjan los estándares o los protocolos de Amazon son investigados y, además, se adoptará contra ellos la acción disciplinaria correspondiente (por ejemplo, una advertencia, un plan de ejecución, una suspensión o la escisión). Consulte el documento técnico de seguridad de la cloud de AWS para obtener información adicional, que se encuentra disponible en http://aws.amazon.com/security. Consulte la norma ISO 27001; Anexo A, dominio 7, para obtener más información. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
	GRM-07.2	¿Los empleados saben qué acciones pueden emprenderse en caso de que realicen alguna infracción? ¿Se explica esta información en las políticas y los procedimientos?	
Gobernanza y administración de riesgos *Efectos de los cambios empresariales o de políticas*	GRM-08.1	¿Los resultados de las evaluaciones incluyen actualizaciones de las políticas, los procedimientos, los estándares y los controles de seguridad a efectos de garantizar que siguen siendo pertinentes y eficaces?	Las actualizaciones de las políticas, los procedimientos, los estándares y los controles de AWS se realizan todos los años de conformidad con el estándar ISO 27001. Consulte la norma ISO 27001 para obtener información adicional. Un auditor independiente ha validado y certificado AWS a fin de confirmar que está en consonancia con la certificación ISO 27001.
Gobernanza y administración de riesgos *Revisiones de las políticas*	GRM-09.1	¿Informa a los inquilinos cuando realiza cambios importantes en las políticas de privacidad o seguridad de la información?	El documento técnico de seguridad de la cloud de AWS y los documentos técnicos sobre riesgos y cumplimiento se encuentran disponibles en http://aws.amazon.com/security y http://aws.amazon.com/compliance, y se actualizan regularmente para reflejar los cambios que se realizan en las políticas de AWS.
	GRM-09.2	¿Realiza revisiones anuales (como mínimo) de sus políticas de privacidad y seguridad?	En los informes SOC de AWS se proporciona más información sobre la revisión de las políticas de seguridad y privacidad.
Gobernanza y administración de riesgos *Evaluaciones*	GRM-10.1	¿Las evaluaciones de riesgos formales están en consonancia con la estructura empresarial y se realizan al menos una vez al año, o en intervalos previstos, a fin de determinar la probabilidad y la repercusión de todos los riesgos identificados, a través de métodos cualitativos y cuantitativos?	De conformidad con el estándar ISO 27001, AWS ha desarrollado un programa de administración de riesgos destinado a mitigar y administrar los riesgos. Un auditor independiente ha validado y certificado AWS a fin de confirmar que está en consonancia con la certificación ISO 27001. Consulte el documento técnico sobre riesgos y conformidad de AWS (disponible en aws.amazon.com/security) para obtener información adicional acerca de la estructura de administración de riesgos de AWS.

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
	GRM-10.2	¿La probabilidad y la repercusión asociadas a los riesgos inherentes y residuales se determinan de manera independiente, teniendo en cuenta todas las categorías de riesgos (por ejemplo, resultados de auditorías, análisis de amenazas y vulnerabilidades y conformidad normativa)?	
Gobernanza y administración de riesgos *Programa*	GRM-11.1	¿Cuenta con un programa documentado que se aplique en toda la organización para administrar los riesgos?	De conformidad con el estándar ISO 27001, AWS cuenta con un programa de administración de riesgos para mitigar y administrar los riesgos. El departamento de administración de AWS ha desarrollado un plan de negocio estratégico que comprende la identificación de riesgos y la ejecución de controles a efectos de mitigar o administrar los riesgos. Este departamento evalúa el plan al menos cada dos años. En este proceso, es preciso que el departamento de administración identifique los riesgos en sus ámbitos de responsabilidad, así como que adopte las medidas apropiadas destinadas a mitigar tales riesgos. Los auditores independientes externos revisan el programa de administración de riesgos de AWS durante las auditorías de nuestra conformidad con PCI DSS, ISO 27001 y FedRAMP.
	GRM-11.2	¿La documentación del programa de administración de riesgos que se aplica en toda la organización es de dominio público?	
Recursos humanos *Devoluciones de recursos*	HRS-01.1	¿Hay sistemas para monitorear las infracciones de privacidad e informar a los inquilinos de inmediato si un evento de privacidad ha afectado a sus datos?	Los clientes de AWS son responsables de monitorear su propio entorno para detectar si se producen violaciones de la privacidad. En los informes SOC de AWS, se ofrece información general acerca de los controles existentes para monitorear el entorno administrado de AWS.
	HRS-01.2	¿Su política de privacidad cumple con los estándares del sector?	
Recursos humanos *Investigación de antecedentes*	HRS-02.1	De conformidad con las leyes locales, los reglamentos, los códigos éticos y las restricciones contractuales, ¿están todos los candidatos, contratistas y terceros participantes sujetos a una verificación de antecedentes?	AWS comprueba los antecedentes penales de conformidad con la legislación aplicable, como parte de las prácticas de preselección de empleados a fin de que estos se adecuen al cargo y al nivel de acceso del empleado a las instalaciones de AWS. En los informes SOC de AWS se ofrece información adicional acerca de los controles disponibles para la investigación de antecedentes.
Recursos humanos *Acuerdos de trabajo*	HRS-03.1	¿Capacita específicamente a los empleados con respecto a su función específica y los controles de seguridad de la información con los que deben cumplir?	De conformidad con el estándar ISO 27001, todos los empleados de AWS realizan una capacitación periódica y específica de su función, que incluye una capacitación sobre seguridad de AWS y que requiere un reconocimiento para completarla. Las auditorías de conformidad se realizan periódicamente a fin de validar que los empleados puedan conocer y seguir las políticas establecidas. Consulte los informes SOC de AWS para obtener más información. Todas las personas que brindan sus servicios en relación con los dispositivos y sistemas de AWS deben firmar un acuerdo de confidencialidad antes de que se les conceda acceso. Además, cuando es contratado por la compañía, el personal tiene que leer y aceptar la Política de Uso Aceptable y la Política del Código de Conducta y Ética Empresarial (Código de Conducta) de Amazon.
	HRS-03.2	¿Documenta los reconocimientos que los empleados obtienen en la capacitación que cursan?	
	HRS-03.3	¿Todos los miembros del personal deben firmar NDA o acuerdos de confidencialidad como condición de empleo para proteger la información del cliente/inquilino?	

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
	HRS-03.4	¿La finalización de la capacitación a tiempo y de forma exitosa se considera un requisito previo para adquirir y mantener el acceso a los sistemas confidenciales?	
	HRS-03.5	¿El personal está capacitado y tiene acceso a programas de concienciación al menos una vez al año?	
Recursos humanos *Terminación del empleo*	HRS-04.1	¿Se cuenta con políticas, procedimientos y directrices documentados para regular el cambio o la terminación del empleo?	El equipo de recursos humanos de AWS define las responsabilidades de administración internas que se deben cumplir para la terminación y el cambio de funciones de los empleados y proveedores. En los informes SOC de AWS se ofrece información adicional.
	HRS-04.2	¿En los procedimientos y las directrices especificados anteriormente se tiene en cuenta la revocación a tiempo del acceso y la devolución de recursos?	El acceso se revoca automáticamente cuando se anula el historial de un empleado en el sistema de Recursos Humanos de Amazon. Cuando se produce un cambio en la función de un empleado, debe aprobarse de forma explícita el acceso continuo al recurso o, de lo contrario, dicho acceso se revocará automáticamente. En los informes SOC de AWS se facilita información adicional acerca de la revocación de acceso a los usuarios. Además, en la sección "Ciclo de vida del empleado" del documento técnico sobre seguridad de AWS se proporciona información adicional. Consulte la norma ISO 27001; Anexo A, dominio 7 para obtener más información. Un auditor independiente ha validado y certificado que AWS cumple con el estándar de certificación ISO 27001.
Recursos Humanos *Dispositivos portátiles/ móviles*	HRS-05.1	¿Se han establecido políticas y procedimientos y aplicado medidas para limitar estrictamente el acceso a sus datos confidenciales y los datos del inquilino desde dispositivos portátiles y móviles, como computadoras portátiles, teléfonos móviles y personal digital assistants (PDA, asistentes digitales personales) que presentan un riesgo más alto que los dispositivos no portátiles, tales como las computadoras de escritorio de las instalaciones de la organización del proveedor?	Los clientes mantienen el control y la responsabilidad de sus datos y de los recursos de medios asociados. Es responsabilidad del cliente administrar los dispositivos móviles de seguridad y el acceso al contenido del cliente.
Recursos humanos *Acuerdos de confidencialidad*	HRS-06.1	¿Se identifican, documentan y revisan en los intervalos previstos los acuerdos de no divulgación o confidencialidad que reflejan las necesidades de la organización en relación con la protección de los datos y los detalles operativos?	El consejo jurídico de Amazon administra y revisa periódicamente los NDA de Amazon a fin de reflejar las necesidades empresariales de AWS.
Recursos Humanos *Funciones y responsabilidades*	HRS-07.1	¿Ofrece a los inquilinos un documento de definición de funciones donde se aclaren las responsabilidades administrativas que usted tiene con respecto a las del inquilino?	En el documento técnico de seguridad de la cloud de AWS y en el documento técnico sobre riesgos y conformidad de AWS se ofrece información detallada acerca de las funciones y responsabilidades de AWS y de nuestros clientes. Los documentos técnicos están disponibles en http://aws.amazon.com/security y http://aws.amazon.com/compliance.

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
Recursos Humanos *Uso aceptable*	HRS-08.1	¿Ofrece documentación acerca de cómo puede utilizar los datos y metadatos de los inquilinos o acerca de cómo acceder a ellos?	AWS cuenta con una política formal de control de acceso que se revisa y actualiza anualmente (o cuando se produce algún cambio importante en el sistema que afecta a la política). La política aborda el propósito, el ámbito de aplicación, las funciones, las responsabilidades y el compromiso de la dirección. AWS emplea el concepto de privilegios mínimos, que solo permite el acceso necesario para que los usuarios desempeñen sus funciones. Los clientes mantienen el control y la responsabilidad de sus datos y de los recursos de medios asociados. Es responsabilidad del cliente administrar los dispositivos móviles de seguridad y el acceso al contenido del cliente. Consulte la norma ISO 27001 y el código de práctica del estándar 27018 para obtener información adicional. Un auditor independiente ha validado y certificado AWS a fin de confirmar que está en consonancia con la certificación ISO 27001 e ISO 27018.
	HRS-08.2	¿Recopila o crea metadatos acerca del uso que el inquilino hace de los datos mediante la utilización de tecnologías de inspección, como los motores de búsqueda, entre otras?	
	HRS-08.3	¿Permite que los inquilinos descarten la opción de que se acceda a sus datos o metadatos a través de tecnologías de inspección?	
Recursos Humanos *Formación/ Concienciación*	HRS-09.1	¿Ofrece algún programa oficial de capacitación basado en las funciones de los empleados para generar conciencia acerca de la seguridad que trate las cuestiones relativas a la administración de los datos y el acceso relacionado con la cloud (es decir, varios inquilinos, nacionalidad, modelo de entrega de la cloud, segregación de funciones, implicaciones y conflictos de intereses) para todas las personas con acceso a los datos del inquilino?	De conformidad con el estándar ISO 27001, todos los empleados de AWS realizan una capacitación periódica sobre la seguridad de la información; para completarla es necesario enviar un acuse de recibo. Las auditorías de conformidad se realizan periódicamente a fin de validar que los empleados puedan conocer y seguir las políticas establecidas. Los auditores independientes externos revisan las funciones y las responsabilidades de AWS durante las auditorías de nuestra conformidad con SOC, PCI DSS, ISO 27001 y FedRAMP.
	HRS-09.2	¿Los administradores y responsables de los datos disponen de la información adecuada acerca de las responsabilidades legales relativas a la seguridad y la integridad de los datos?	
Recursos Humanos *Responsabilidad del usuario*	HRS-10.1	¿Los usuarios son conscientes de sus responsabilidades en cuanto a mantener la concienciación y el cumplimiento con respecto a las políticas, los procedimientos y los estándares de seguridad y las disposiciones normativas aplicables?	AWS ha implementado varios métodos de comunicación interna a escala mundial para ayudar a que los empleados conozcan las funciones y las responsabilidades individuales y para comunicar eventos importantes de manera puntual. Estos métodos incluyen programas de capacitación y orientación para los empleados recién contratados, además de mensajes de correo electrónico y la publicación de información a través de la intranet de Amazon. Consulte la norma ISO 27001, anexo A, dominios 7 y 8. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001. Además, en el documento técnico de seguridad de la cloud de AES se proporciona información adicional. Dicho documento se encuentra disponible en http://aws.amazon.com/security.
	HRS-10.2	¿Los usuarios son conscientes de las responsabilidades que tienen en lo que respecta a mantener un entorno de trabajo seguro y protegido?	
	HRS-10.3	¿Los usuarios son conscientes de las responsabilidades que tienen relacionadas con dejar un equipo desatendido de manera segura?	

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
Recursos Humanos *Espacio de trabajo*	HRS-11.1	¿Los procedimientos y las políticas de administración de datos abordan los conflictos de intereses de inquilinos y de nivel de servicio?	Las políticas de administración de datos de AWS cumplen con el estándar ISO 27001. Consulte la norma ISO 27001, anexo A, dominios 8 y 9. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001. En los informes SOC de AWS se ofrece información adicional acerca de las actividades de control específicas que lleva a cabo AWS para prevenir el acceso no autorizado a los recursos de AWS. AWS ha identificado las categorías de eventos auditables en sus sistemas y dispositivos del sistema de AWS. Los equipos de servicio configuran las características de auditoría para registrar continuamente los eventos relacionados con la seguridad de acuerdo con los requisitos. Los registros de auditoría contienen una serie de elementos de datos para admitir los requisitos de análisis necesarios. Además, el equipo de seguridad de AWS u otros equipos apropiados puede utilizar los registros de auditoría para realizar inspecciones o análisis por demanda, o como respuesta a eventos relacionados con la seguridad o que repercuten en el negocio.
	HRS-11.2	¿Los procedimientos y las políticas de administración de datos incluyen alguna función de integridad del software o de auditoría de manipulaciones para casos de acceso no autorizado a los datos del inquilino?	
	HRS-11.3	¿La infraestructura de administración de la máquina virtual incluye alguna función de integridad del software o de auditoría de manipulaciones para detectar cambios en la compilación o configuración de la máquina virtual?	
Identity & Access Management *Acceso de herramientas de auditoría*	IAM-01.1	¿Restringe, registra y monitorea el acceso a los sistemas de administración de seguridad de la información? (Por ejemplo, hipervisores, firewalls, escáneres de vulnerabilidades, analizadores de protocolos de red, API, etc.)	De conformidad con los estándares ISO 27001, AWS ha establecido políticas y procedimientos formales para delinear los estándares mínimos de acceso lógico a los recursos de AWS. En los informes SOC de AWS, se describen los controles existentes para administrar la provisión de acceso a los recursos de AWS. Consulte el documento técnico de seguridad de la cloud de AWS para obtener información adicional, que se encuentra disponible en http://aws.amazon.com/security.
	IAM-01.2	¿Monitorea y registra el acceso privilegiado a los sistemas de administración de seguridad de la información (nivel de administrador)?	AWS ha identificado las categorías de eventos auditables en sus sistemas y dispositivos del sistema de AWS. Los equipos de servicio configuran las características de auditoría para registrar continuamente los eventos relacionados con la seguridad de acuerdo con los requisitos. El sistema de almacenamiento de registros está diseñado para ofrecer un sistema de alta escalabilidad y disponibilidad que aumenta automáticamente la capacidad a medida que crece la necesidad de almacenar registros. Los registros de auditoría contienen una serie de elementos de datos para admitir los requisitos de análisis necesarios. Además, el equipo de seguridad de AWS u otros equipos apropiados puede utilizar los registros de auditoría para realizar inspecciones o análisis por demanda, o como respuesta a eventos relacionados con la seguridad o que repercuten en el negocio. El personal designado de los equipos de AWS recibe alertas automatizadas en caso de que se produzca un error en el procesamiento de auditoría. Entre los errores en el procesamiento de auditoría se incluyen errores de software y hardware. Cuando se recibe una alerta, el personal de guardia emite un vale de problema y hace un seguimiento del evento hasta que se resuelve. Los auditores independientes externos revisan los procesos de monitoreo y registro de AWS como parte de nuestro programa continuado de conformidad con SOC, PCI DSS, ISO 27001 y FedRAMP.
Identity & Access Management *Política sobre el acceso de usuarios*	IAM-02.1	¿Cuenta con controles que garanticen la eliminación oportuna del acceso de los sistemas que dejan de ser necesarios para los fines empresariales?	En los informes SOC de AWS se facilita información adicional acerca de la revocación de acceso a los usuarios. Además, en la sección "Employee Lifecycle" (ciclo de vida del empleado) del documento técnico sobre seguridad de AWS se proporciona información adicional. Consulte la norma ISO 27001; Anexo A, dominio 9 para obtener más información. Un auditor independiente ha validado y certificado que AWS cumple con el estándar de certificación ISO 27001.

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
	IAM-02.2	¿Ofrece métricas que realizan un seguimiento de la agilidad con la que puede revocar el acceso de los sistemas que dejan de ser necesarios para los fines empresariales?	
Identity & Access Management *Acceso de los puertos de configuración y diagnóstico*	IAM-03.1	¿Utiliza redes seguras dedicadas para ofrecer acceso de admnistración a la infraestructura del servicio de la cloud?	Los controles existentes limitan el acceso a sistemas y datos, además de estipular que el acceso a los sistemas o datos se restrinja y monitoree según la política de acceso de AWS. Asimismo, los datos de los clientes y las instancias de servidor se aíslan de forma lógica de otros clientes de manera predeterminada. Un auditor independiente examina los controles de acceso de usuarios privilegiados en el marco de las auditorías de AWS SOC, ISO 27001, PCI, ITAR y FedRAMP de AWS.
Identity & Access Management *Políticas y procedimientos*	IAM-04.1	¿Administra y almacena la información sobre la identidad de todo el personal que tiene acceso a la infraestructura de TI, incluido su nivel de acceso?	
	IAM-04.2	¿Administra y almacena la información sobre la identidad de usuarios de todo el personal que tiene acceso a las redes, incluido su nivel de acceso?	
Identity & Access Management *Segregación de funciones*	IAM-05.1	¿Ofrece documentación a los inquilinos acerca de cómo mantener la segregación de funciones dentro de la oferta del servicio de la cloud?	Los clientes tienen la capacidad de administrar las segregaciones de funciones de los recursos de AWS. A nivel interno, AWS cumple con el estándar ISO 27001 en lo relativo a la administración de la segregación de funciones. Consulte la norma ISO 27001, anexo A, dominio 6, para obtener información adicional. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
Identity & Access Management *Restricción de acceso al código fuente*	IAM-06.1	¿Se aplican controles para prevenir el acceso no autorizado al código fuente de la aplicación, el programa o el objeto, así como para garantizar que dicho acceso se restrinja solo a personal autorizado?	De conformidad con los estándares ISO 27001, AWS ha establecido políticas y procedimientos formales para delinear los estándares mínimos de acceso lógico a los recursos de AWS. En los informes SOC de AWS, se describen los controles existentes para administrar la provisión de acceso a los recursos de AWS. Consulte el documento técnico de información general sobre los procesos de seguridad de AWS para obtener información adicional, que se encuentra disponible en http://aws.amazon.com/security.
	IAM-06.2	¿Se aplican controles para prevenir el acceso no autorizado al código fuente de la aplicación, el programa o el objeto, así como para garantizar que dicho acceso se restrinja solo a personal autorizado?	
Identity & Access Management *Acceso de terceros*	IAM-07.1	¿Ofrece alguna función de recuperación de desastres para casos con múltiples errores?	AWS ofrece a los clientes la flexibilidad necesaria para colocar las instancias y almacenar datos en varias regiones geográficas, así como en zonas de disponibilidad múltiples dentro de cada región. Cada zona de disponibilidad está diseñada como una zona de error independiente. En caso de error, los procesos automatizados desvían el tráfico de datos del cliente de la zona afectada. En los informes SOC de AWS se ofrece información adicional. En el estándar ISO 27001, Anexo A, dominio 15 se ofrece más información. Un auditor independiente ha validado y certificado AWS a fin de confirmar que está en consonancia con la certificación ISO 27001.
	IAM-07.2	¿Realiza un monitoreo de la continuidad del servicio con los proveedores ascendentes por si falla su proveedor?	
	IAM-07.3	¿Dispone de más de un proveedor para cada servicio del que depende?	

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
	IAM-07.4	¿Ofrece acceso a resúmenes de continuidad y redundancia operativa que incluyan los servicios de los que depende?	
	IAM-07.5	¿Brinda al inquilino la posibilidad de declarar un desastre?	
	IAM-07.6	¿Ofrece alguna opción de que pueda activar el inquilino?	
	IAM-07.7	¿Comparte con sus inquilinos los planes de redundancia y continuidad empresarial?	
Identity & Access Management *Autorización y restricción de acceso de usuarios*	IAM-08.1	¿Documenta cómo concede y aprueba el acceso a los datos del inquilino?	Los clientes de AWS mantienen el control y la propiedad de sus datos. Los controles existentes limitan el acceso a sistemas y datos, además de estipular que el acceso a los sistemas o datos se restrinja y monitoree. Asimismo, los datos de los clientes y las instancias de servidor se aíslan de forma lógica de otros clientes de manera predeterminada. Un auditor independiente examina los controles de acceso de usuarios privilegiados en el marco de las auditorías de AWS SOC, ISO 27001, PCI, ITAR y FedRAMP de AWS.
	IAM-08.2	¿Dispone de un método para alinear las metodologías de clasificación de los datos de proveedores e inquilinos a efectos de control de acceso?	
Identity & Access Management *Autorización de acceso de usuarios*	IAM-09.1	¿La gerencia de su empresa aprovisiona las autorizaciones y restricciones del acceso de los usuarios (por ejemplo, empleados, contratistas, clientes [inquilinos], socios comerciales o proveedores) antes de que estos puedan tener acceso a los componentes de red, los sistemas de infraestructura y las aplicaciones (físicas y virtuales) administradas o de su propiedad?	Se crean identificadores únicos de usuario como parte del proceso de flujo de trabajo de incorporación en el sistema de administración de recursos humanos de AWS. El proceso de concesión de acceso a los dispositivos permite garantizar identificadores únicos para los dispositivos. Ambos procesos incluyen la aprobación del gerente para establecer la cuenta de usuario o el dispositivo. Los autenticadores iniciales se entregan al usuario en persona y a los dispositivos como parte del proceso de aprovisionamiento. Los usuarios internos pueden asociar claves públicas SSH con su cuenta. Los autenticadores de cuentas del sistema se proporcionan al solicitante como parte del proceso de creación de cuentas una vez que se verifica la identidad del solicitante.
	IAM-09.2	¿Ofrece, a pedido, acceso a los usuarios (por ejemplo, empleados, contratistas, clientes [inquilinos], socios comerciales o proveedores) a los datos y los componentes de red, los sistemas de infraestructura y las aplicaciones (físicas y virtuales) administradas o de su propiedad?	AWS aplicó controles para solucionar la amenaza de acceso confidencial no apropiado. Todas las certificaciones y acreditaciones independientes evalúan los controles lógicos de detección y prevención de acceso. Asimismo, las evaluaciones de riesgo periódicas se centran en la forma de controlar y monitorear el acceso confidencial.
Identity & Access Management *Revisiones de acceso de usuarios*	IAM-10.1	¿Requiere al menos una certificación anual de los derechos de todos los administradores y usuarios del sistema (excluidos los usuarios de cuyo mantenimiento se encargan los inquilinos)?	De conformidad con el estándar ISO 27001, todas las concesiones de acceso se revisan periódicamente; se requieren reaprobaciones explícitas o, de lo contrario, el acceso al recurso se revoca de inmediato. Los controles específicos para las revisiones de acceso de usuarios se describen en los informes SOC. Las excepciones de los controles de derechos de usuario se documentan en los informes SOC. Consulte la norma ISO 27001; Anexo A, Dominio 9, para obtener información adicional.

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
	IAM-10.2	Si se observa que los usuarios tienen derechos inapropiados, ¿se registran todas las acciones de reparación y certificación?	Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
	IAM-10.3	En caso de que se haya permitido el acceso inapropiado a los datos del inquilino, ¿compartirá los informes de certificación y reparación de los derechos de usuario con los inquilinos?	
Identity & Access Management *Revocación de acceso a usuarios*	IAM-11.1	¿Se aplican de manera oportuna la cancelación del aprovisionamiento, la revocación o la modificación del acceso de los usuarios a los sistemas, los recursos de información y los datos de la organización tras producirse algún cambio en el estado de los empleados, los contratistas, los clientes, los socios empresariales o terceros implicados?	El acceso se revoca automáticamente cuando se anula el historial de un empleado en el sistema de recursos humanos de Amazon. Cuando se produce un cambio en la función de un empleado, ha de aprobarse de forma explícita el acceso continuado al recurso o, de lo contrario, dicho acceso se revocará automáticamente. En los informes SOC de AWS se facilita información adicional acerca de la revocación de acceso a los usuarios. Además, en la sección "Employee Lifecycle" (ciclo de vida del empleado) del documento técnico sobre seguridad de AWS se proporciona información adicional. Consulte la norma ISO 27001; Anexo A, dominio 9 para obtener más información. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
	IAM-11.2	¿Se prevé algún cambio de estado en el acceso de los usuarios para incluir la terminación del empleo, el contrato o el acuerdo, el cambio de empleo o la transferencia dentro de la organización?	
Identity & Access Management *Credenciales de ID del usuario*	IAM-12.1	¿Admite el uso o la integración con soluciones de Single Sign On (SSO, inicio de sesión único) basadas en clientes existentes en su servicio?	El servicio AWS Identity and Access Management (IAM) ofrece la identidad federada en la consola de administración de AWS. La autenticación multifactor es una característica opcional que el cliente puede utilizar. Consulte el sitio web de AWS http://aws.amazon.com/mfa para obtener información adicional. AWS Identity and Access Management (IAM) es compatible con la identidad federada para el acceso delegado a la consola de administración de AWS o las API de AWS. A través de la identidad federal, las identidades externas (usuarios federados) obtienen acceso seguro a los recursos de su cuenta de AWS sin tener que crear usuarios de IAM. Estas identidades externas las puede proporcionar su proveedor de identidades corporativas (como Microsoft Active Directory o AWS Directory Service) o un proveedor de identidades web, como Amazon Cognito, Login with Amazon, Facebook, Google o cualquier proveedor compatible con OpenID Connect (OIDC).
	IAM-12.2	¿Utiliza estándares abiertos para delegar las funciones de autenticación a los inquilinos?	
	IAM-12.3	¿Admite estándares de identidades federadas (SAML, SPML, WS-Federation, etc.) como medio para autenticar/autorizar usuarios?	
	IAM-12.4	¿Dispone de una función de punto de aplicación de políticas (por ejemplo, XACML) para imponer restricciones políticas y legales regionales en relación con el acceso de los usuarios?	
	IAM-12.5	¿Cuenta con un sistema de administración de identidades que admita los derechos basados tanto en contextos como en funciones sobre los datos (es decir, que permita la clasificación de los datos de un inquilino)?	

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
	IAM-12.6	¿Ofrece a los inquilinos opciones sólidas de autenticación (multifactor) como certificados digitales, tokens, datos biométricos, etc. para el acceso de los usuarios?	
	IAM-12.7	¿Permite que los inquilinos utilicen servicios de garantía de identidades de terceros?	
	IAM-12.8	¿Respalda el cumplimiento de la política de contraseñas (longitud mínima, antigüedad, historial, complejidad) y de bloqueo de cuentas (límite de bloqueos, duración del bloqueo)?	AWS Identity and Access Management (IAM) permite a los clientes controlar de forma segura el acceso de sus usuarios a servicios y recursos de AWS. Encontrará información adicional sobre IAM en el siguiente sitio web: https://aws.amazon.com/iam/. En los informes SOC de AWS, se ofrece información acerca de las actividades de control específicas que ejecuta AWS.
	IAM-12.9	¿Permite que los inquilinos/clientes definan las políticas de bloqueo de cuentas y contraseñas de sus propias cuentas?	
	IAM-12.10	¿Respalda la capacidad de forzar el cambio de contraseña del primer inicio de sesión?	
	IAM-12.11	¿Cuenta con algún mecanismo para desbloquear cuentas que se bloquearon (por ejemplo, autoservicio por correo electrónico, preguntas definidas sobre los desafíos de seguridad, desbloqueo manual)?	
Identity & Access Management *Acceso a programas de utilidades*	IAM-13.1	¿Se restringen y monitorean adecuadamente las utilidades que pueden administrar particiones virtualizadas (como apagar, clonar, etc.)?	De conformidad con los estándares ISO 27001, las utilidades del sistema se restringen y monitorean correctamente. En los informes SOC de AWS, se ofrece información acerca de las actividades de control específicas que ejecuta AWS. Consulte el documento técnico de información general sobre los procesos de seguridad de AWS para obtener información adicional, que se encuentra disponible en http://aws.amazon.com/security.
	IAM-13.2	¿Tiene capacidad para detectar ataques dirigidos directamente a la infraestructura virtual (por ejemplo, procesamiento con shims, Blue Pill, Hyper jumping, etc.)?	
	IAM-13.3	¿Los controles técnicos previenen los ataques destinados a la infraestructura virtual?	

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
Seguridad de virtualización e infraestructura *Detección de intrusiones y registros de auditoría*	IVS-01.1	¿Se utilizan las herramientas de network intrusion detection (IDS, detección de intrusiones de red) y de integridad de los archivos (host) para facilitar la detección oportuna, la investigación mediante análisis de la causa raíz y la respuesta a las incidencias?	El programa de respuesta a incidencias de AWS (detección, investigación y respuesta a incidencias) se ha desarrollado de conformidad con el estándar ISO 27001 y para controlar que las utilidades del sistema se estén restringiendo y monitoreando de forma apropiada. En los informes SOC de AWS, se ofrece información adicional acerca de los controles disponibles para restringir el acceso al sistema. Consulte el documento técnico de información general sobre los procesos de seguridad de AWS para obtener información adicional, que se encuentra disponible en http://aws.amazon.com/security.
	IVS-01.2	¿Está restringido a personal autorizado el acceso físico y lógico de los usuarios a los registros de auditoría?	
	IVS-01.3	¿Puede demostrar la diligencia debida en el mapeo de las normativas o los estándares de acuerdo con sus controles, su arquitectura y sus procesos?	
	IVS-01.4	¿Los registros de auditorías están almacenados y se conservan en un lugar centralizado?	De conformidad con los estándares ISO 27001, los sistemas de información de AWS utilizan relojes internos del sistema sincronizados a través del Network Time Protocol (NTP, protocolo de tiempo de redes). Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001. AWS utiliza sistemas automáticos de monitoreo para ofrecer un alto nivel de rendimiento y disponibilidad de los servicios. El monitoreo proactivo se encuentra disponible a través de una serie de herramientas en línea destinadas tanto para uso interno como externo. Los sistemas de AWS disponen de una gran variedad de recursos para poder monitorear las principales métricas operativas. Las alarmas se configuran para notificar al personal de operaciones y administración cuándo las métricas operativas clave superan los umbrales de advertencias anticipadas. Se utiliza un programa de asistencia de guardia a fin de que este personal esté siempre disponible para solucionar los problemas de funcionamiento. Incluye además un sistema de localización de personas para que las alarmas se comuniquen al personal de operaciones de forma rápida y fiable. Consulte el documento técnico de seguridad de la cloud de AWS para obtener información adicional, que se encuentra disponible en http://aws.amazon.com/security.
	IVS-01.5	¿Los registros de las auditorías se revisan periódicamente para ver si hay eventos de seguridad (por ejemplo, con herramientas automatizadas)?	
Seguridad de virtualización e infraestructura *Detección de cambios*	IVS-02.1	¿Registra e informa los cambios realizados en las imágenes de la máquina virtual, independientemente de su estado de funcionamiento (por ejemplo, suspendida, apagada o en funcionamiento)?	Las máquinas virtuales se asignan a los clientes como parte del servicio de EC2. Los clientes mantienen el control de los recursos que se utilizan y dónde estos residen. Consulte el sitio web de AWS http://aws.amazon.com para obtener información adicional.
	IVS-02.2	¿Los cambios que se realizan en las maquinas virtuales o el cambio de lugar de una imagen y la subsiguiente validación de su integridad están automáticamente disponibles para los clientes a través de métodos electrónicos (por ejemplo, portales o alertas)?	

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
Seguridad de virtualización e infraestructura *Sincronización del reloj*	IVS-03.1	¿Utiliza un protocolo de servicio temporal sincronizado (por ejemplo, NTP) para garantizar que todos los sistemas tengan una referencia temporal en común?	De conformidad con los estándares ISO 27001, los sistemas de información de AWS utilizan relojes internos del sistema sincronizados a través del Network Time Protocol (NTP, protocolo de tiempo de redes). Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
Seguridad de virtualización e infraestructura *Planificación de capacidad y recursos*	IVS-04.1	¿Proporciona documentación con respecto a qué niveles de sobresuscripción del sistema (red, almacenamiento, memoria, E/S, etc.) mantiene y en qué circunstancias o situaciones?	La información sobre los límites de servicio de AWS y sobre cómo solicitar un aumento en determinados servicios está disponible en el sitio web de AWS, en http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html. AWS administra los datos de capacidad y utilización de conformidad con el estándar ISO 27001. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
	IVS-04.2	¿Restringe el uso de las funciones de sobresuscripción de la memoria existentes en el hipervisor?	
	IVS-04.3	¿En los requisitos de capacidad de su sistema se tienen en cuenta las necesidades de capacidad actuales, proyectadas y anticipadas de todos los sistemas usados para proporcionar servicios a los inquilinos?	
	IVS-04.4	¿El rendimiento del sistema se monitorea y ajusta para cumplir constantemente con los requisitos regulatorios, contractuales y comerciales de todos los sistemas usados para proporcionar servicios a los inquilinos?	
Seguridad de virtualización e infraestructura *Administración; administración de vulnerabilidades*	IVS-05.1	¿Los servicios o las herramientas de evaluación de la vulnerabilidad de la seguridad se ajustan a las tecnologías de virtualización que se utilizan (por ejemplo, tienen en cuenta la virtualización)?	Amazon EC2 actualmente utiliza una versión bastante personalizada del hipervisor Xen. Los equipos de intrusión internos y externos evalúan regularmente el hipervisor para detectar las vulnerabilidades nuevas y existentes y los vectores de ataque. Este hipervisor está perfectamente adaptado para mantener un fuerte aislamiento entre las máquinas virtuales invitadas. Durante las evaluaciones y auditorías, los auditores independientes evalúan con regularidad la seguridad del hipervisor Xen de AWS. Se realizan periódicamente análisis de vulnerabilidades internos y externos del sistema operativo host, la aplicación web y las bases de datos del entorno de AWS con diversas herramientas. Las prácticas de escaneo y corrección de vulnerabilidades se revisan periódicamente como parte del programa continuado de AWS de conformidad con PCI DSS y FedRAMP.
Seguridad de virtualización e infraestructura *Seguridad de la red*	IVS-06.1	Para las ofertas de Infrastructure as a Service (IaaS, infraestructura como servicio), ¿ofrece a los clientes orientación acerca de cómo crear una equivalencia de arquitectura de seguridad por capas usando una solución virtualizada?	En el sitio web de AWS se ofrecen directrices acerca de cómo crear una arquitectura de seguridad por capas en una serie de documentos técnicos que se encuentran disponibles en el sitio web público de AWS, en http://aws.amazon.com/documentation/.

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
	IVS-06.2	¿Actualiza periódicamente los diagramas de arquitectura de la red que incluyen flujos de datos entre las zonas y los dominios de seguridad?	Los dispositivos de protección perimetral que emplean conjuntos de reglas, access control lists (ACL, listas de control de acceso) y configuraciones garantizan el flujo de información entre el entramado de la red. En Amazon existen varios entramados de red y todos están separados por dispositivos que controlan el flujo de información entre dichos entramados. El flujo de información entre los entramados se establece mediante autorizaciones aprobadas en forma de listas de control de acceso (ACL), que residen en estos dispositivos. Estos dispositivos controlan el flujo de información entre los entramados conforme lo estipulan estas ACL. El personal adecuado define y aprueba las ACL, que se administran e implementan mediante la herramienta de administración de ACL de AWS. El equipo de seguridad de la información de Amazon aprueba estas ACL. Las listas de control de acceso entre entramados de la red y los conjuntos de reglas del firewall aprobados restringen el flujo de información a determinados servicios de los sistemas de información. Los conjuntos de reglas y las listas de control de acceso se revisan y aprueban, y se envían automáticamente a los dispositivos de protección perimetral de forma periódica (al menos cada 24 horas) para garantizar que estén actualizados. Los auditores independientes externos revisan periódicamente la administración de la red de AWS como parte de nuestro programa continuado de conformidad con SOC, PCI DSS, ISO 27001 y FedRAMP[sm]. AWS implementa privilegios mínimos en todos los componentes de su infraestructura. AWS prohíbe todos los puertos y protocolos que no tengan un fin empresarial específico. AWS sigue un proceso riguroso para la implementación mínima solamente de las características y funciones que son esenciales para el uso del dispositivo. Se realiza un escaneo de la red y se corrigen todos los puertos o protocolos innecesarios que están en uso. Se realizan periódicamente análisis de vulnerabilidades internos y externos del sistema operativo host, la aplicación web y las bases de datos del entorno de AWS con diversas herramientas. Las prácticas de escaneo y corrección de vulnerabilidades se revisan periódicamente como parte del programa continuado de AWS de conformidad con PCI DSS y FedRAMP.
	IVS-06.3	¿Revisa periódicamente la adecuación del acceso permitido/la conectividad (por ejemplo, reglas de firewall) entre las zonas/los dominios de seguridad de la red?	
	IVS-06.4	¿Todas las listas de control de acceso a los firewall están documentadas con una justificación comercial?	
Seguridad de virtualización e infraestructura *Controles básicos y de protección del SO*	IVS-07.1	¿Los sistemas operativos se protegen para proporcionar solo los puertos, protocolos y servicios necesarios para satisfacer las necesidades comerciales mediante controles técnicos (por ejemplo, antivirus, monitoreo de integridad de archivos y registro) como parte de la plantilla o el estándar de creación de referencia?	
Seguridad de virtualización e infraestructura *Entornos de producción y de no producción*	IVS-08.1	En caso de que se trate de ofertas de Software as a Service (SaaS, software como servicio) y de Platform as a Service (PaaS, plataforma como servicio), ¿ofrece a los inquilinos entornos independientes para los procesos de producción y pruebas?	Los clientes de AWS tienen la posibilidad y la responsabilidad de crear y mantener los entornos de producción y pruebas. En el sitio web de AWS se ofrecen directrices acerca de cómo crear un entorno que utilice los servicios de AWS, disponible en http://aws.amazon.com/documentation/.
	IVS-08.2	Para las ofertas de Infrastructure as a Service (IaaS, infraestructura como servicio), ¿ofrece orientación a los inquilinos acerca de cómo crear entornos adecuados de producción y pruebas?	
	IVS-08.3	¿Separa lógica y físicamente los entornos de producción y de no producción?	Los clientes de AWS mantienen la responsabilidad de administrar su propia segmentación de red de acuerdo con sus requisitos definidos. Internamente, la segmentación de la red de AWS está en sintonía con los estándares ISO 27001. Consulte la norma ISO 27001, Anexo A, Dominio 13, para obtener información adicional. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
Seguridad de virtualización e infraestructura *Segmentación*	IVS-09.1	¿Los entornos de red y del sistema están protegidos por un firewall o un firewall virtual a fin de garantizar que se satisfacen las necesidades de seguridad del cliente y de la empresa?	

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
	IVS-09.2	¿Los entornos de red y del sistema están protegidos por un firewall o un firewall virtual a fin de garantizar el cumplimiento con los requisitos legislativos, regulatorios y contractuales?	
	IVS-09.3	¿Los entornos de red y del sistema están protegidos por un firewall o un firewall virtual a fin de garantizar la separación de los entornos de producción y de no producción?	
	IVS-09.4	¿Los entornos de red y del sistema están protegidos por un firewall o un firewall virtual a fin de garantizar la protección y el aislamiento de los datos confidenciales?	
Seguridad de virtualización e infraestructura *Seguridad de las máquinas virtuales - vMotion Data Protection*	IVS-10.1	¿Los canales de comunicación asegurados y cifrados se usan para migrar servidores, aplicaciones o datos físicos a los servidores virtuales?	AWS les ofrece a los clientes la posibilidad de utilizar su propio mecanismo de cifrado prácticamente para todos los servicios, incluidos S3, EBS y EC2. También se cifran las sesiones de VPC.
	IVS-10.2	¿Usa una red separada de las redes del nivel de producción para migrar aplicaciones, datos o servidores físicos a los servidores virtuales?	Los clientes de AWS preservan el control y la titularidad de sus propios datos. AWS les ofrece a los clientes la posibilidad de mantener y desarrollar entornos productivos y no productivos. Es responsabilidad del cliente garantizar que los datos de producción no se repliquen en entornos no productivos.
Seguridad de virtualización e infraestructura *Seguridad del VMM - Protección del hipervisor*	IVS-11.1	¿Restringe el acceso del personal a todas las funciones de administración del hipervisor o consolas de administración para los sistemas en los que se alojan sistemas virtualizados que se basan en el principio de privilegios mínimos y soporte a través de controles técnicos (por ejemplo, autenticación de dos factores, seguimiento de auditorías, filtrado de direcciones IP, firewalls y comunicaciones encapsuladas en TLS para las consolas de administración)?	AWS emplea el concepto de privilegios mínimos, que solo permite el acceso necesario para que los usuarios desempeñen sus funciones. Cuando se crean cuentas de usuario, estas tienen un acceso mínimo. Un acceso superior a los privilegios mínimos requiere la autorización correspondiente. Consulte los informes SOC de AWS para obtener más información sobre los controles de acceso.
Seguridad de virtualización e infraestructura *Seguridad de la conexión inalámbrica*	IVS-12.1	¿Se han establecido políticas y procedimientos, y se han configurado y aplicado mecanismos para proteger los perímetros del entorno de red inalámbrica y restringir el tráfico inalámbrico no autorizado?	AWS cuenta con políticas, procedimientos y mecanismos destinados a proteger el entorno de red. Los auditores independientes externos revisan los controles de seguridad de AWS durante las auditorías de nuestra conformidad con SOC, PCI DSS, ISO 27001 y FedRAMP.

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
	IVS-12.2	¿Se han establecido políticas y procedimientos y se han aplicado mecanismos para garantizar que la configuración de seguridad inalámbrica está habilitada con un cifrado reforzado a efectos de autenticación y transmisión, de forma que se reemplace la configuración predeterminada del proveedor? (Por ejemplo, claves de cifrado, contraseñas, enlaces comunitarios SNMP)	
	IVS-12.3	¿Se han establecido políticas y procedimientos, y se han aplicado mecanismos para proteger los entornos de red inalámbrica y detectar la presencia de dispositivos de red no autorizados para una desconexión oportuna de la red?	
Seguridad de virtualización e infraestructura *Arquitectura de la red*	IVS-13.1	¿En sus diagramas de arquitectura de la red se identifican claramente los entornos de alto riesgo y los flujos de datos que pueden tener un impacto legal en el cumplimiento?	Los clientes de AWS mantienen la responsabilidad de administrar su propia segmentación de red de acuerdo con sus requisitos definidos. Internamente, la segmentación de la red de AWS está en sintonía con el estándar ISO 27001. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
	IVS-13.2	¿Implementa medidas técnicas y aplica estrictas técnicas de defensa (por ejemplo, análisis profundo de paquetes, limitación controlada del tráfico y uso de métodos de blackholing) para la detección y la proporción de respuestas a tiempo a los ataques basados en la red y asociados con los patrones de tráfico anómalo de ingreso o egreso (por ejemplo, suplantación de MAC y ataques a ARP de tipo poisoning) o ataques distribuidos por denial-of-service (DDoS, denegación de servicio)?	AWS Security analiza con regularidad todas las direcciones IP de punto de enlace de los servicios expuestas a Internet a fin de detectar vulnerabilidades (estos análisis no incluyen las instancias de los clientes). AWS Security notifica al respecto a las partes correspondientes para remediar todas las vulnerabilidades detectadas. Asimismo, empresas de seguridad independientes realizan con regularidad evaluaciones de amenazas de vulnerabilidades externas. Los resultados y las recomendaciones derivados de estas evaluaciones se clasifican y, además, se entregan a los equipos directivos de AWS. Asimismo, el entorno de control de AWS está sujeto a evaluaciones de riesgos internas y externas de carácter regular. AWS colabora con auditores independientes y organismos de certificación externos para revisar y probar el entorno de control global de AWS. Los auditores independientes externos revisan los controles de seguridad de AWS durante las auditorías de nuestra conformidad con SOC, PCI DSS, ISO 27001 y FedRAMP.

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
Interoperabilidad y portabilidad *API*	IPY-01	¿Publica una lista de todas las API disponibles en el servicio e indica cuáles se consideran estándar y cuáles están personalizadas?	Podrá encontrar más información sobre las API de AWS en el sitio web de AWS, en https://aws.amazon.com/documentation/. De conformidad con los estándares ISO 27001, AWS ha establecido políticas y procedimientos formales para delinear los estándares mínimos de acceso lógico a los recursos de AWS. En los informes SOC de AWS, se describen los controles existentes para administrar la provisión de acceso a los recursos de AWS. Consulte el documento técnico de seguridad de la cloud de AWS para obtener información adicional, que se encuentra disponible en http://aws.amazon.com/security.
Interoperabilidad y portabilidad *Solicitud de datos*	IPY-02	¿Los datos del cliente no estructurados están disponibles a pedido en un formato estándar de la industria (por ejemplo, .doc, .xls o .pdf)?	
Interoperabilidad y portabilidad *Políticas y cuestiones legales*	IPY-03.1	¿Proporciona políticas y procedimientos (por ejemplo, acuerdos de nivel de servicios) que regulen el uso de API para la interoperabilidad entre su servicio y las aplicaciones de terceros?	
	IPY-03.2	¿Proporciona políticas y procedimientos (por ejemplo, acuerdos de nivel de servicios) que regulen la migración de datos de la aplicación hacia y desde su servicio?	Los clientes mantienen el control y la titularidad de su contenido. Los clientes pueden decidir de qué modo desean migrar las aplicaciones y el contenido hacia dentro o fuera de la plataforma de AWS según sus necesidades.
Interoperabilidad y portabilidad *Protocolos estandarizados de red*	IPY-04.1	¿Es posible realizar la importación y exportación de datos y la administración de servicios mediante protocolos estandarizados de red seguros (por ejemplo, texto cifrado y autenticado) y aceptados en la industria?	AWS permite que los clientes extraigan y añadan datos en los servicios de almacenamiento de AWS. Consulte http://aws.amazon.com/choosing-a-cloud-platform para obtener más información sobre las opciones de almacenamiento.
	IPY-04.2	¿Proporciona a los clientes (inquilinos) documentación en la que se detallen los estándares de los protocolos de interoperabilidad y portabilidad de la red que están involucrados?	
Interoperabilidad y portabilidad *Virtualización*	IPY-05.1	¿Usa una plataforma de virtualización reconocida de la industria y formatos de virtualización estándares (por ejemplo, OVF) para garantizar la interoperabilidad?	Amazon EC2 actualmente utiliza una versión bastante personalizada del hipervisor Xen. Los equipos de intrusión internos y externos evalúan regularmente el hipervisor para detectar las vulnerabilidades nuevas y existentes y los vectores de ataque. Este hipervisor está perfectamente adaptado para mantener un fuerte aislamiento entre las máquinas virtuales invitadas. Durante las evaluaciones y auditorías, los auditores independientes evalúan con regularidad la seguridad del hipervisor Xen de AWS. Consulte el documento técnico de seguridad de la cloud de AWS para obtener información adicional, que se encuentra disponible en http://aws.amazon.com/security.
	IPY-05.2	¿Se realizaron cambios personalizados documentados en algún hipervisor en uso y todos los enlaces de virtualización específicos de las soluciones están disponibles para que el cliente los revise?	

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
Seguridad móvil *Antimalware*	MOS-01	¿Proporciona capacitación sobre antimalware específica para los dispositivos móviles como parte de su capacitación de concienciación sobre la seguridad de la información?	El programa, los procesos y los procedimientos de AWS para administrar el antivirus y el software malicioso están en consonancia con el estándar ISO 27001. Consulte la norma ISO 27001, Anexo A, Dominio 12, para obtener información adicional.
Seguridad móvil *Tiendas de aplicaciones*	MOS-02	¿Documenta y publica las listas de las tiendas de aplicaciones aprobadas para los dispositivos móviles desde los que se accede a sistemas o datos de la compañía o en los que se almacena dicha información?	AWS ha establecido un marco y políticas de seguridad de la información en los que se ha integrado de forma eficiente el marco certificable ISO 27001 sobre la base de los controles de ISO 27002, los Principios de los Servicios de Confianza del American Institute of Certified Public Accountants (AICPA), el PCI DSS v3.1 y la Publicación 800-53 del National Institute of Standards and Technology (NIST, Instituto Nacional de Estándares y Tecnología) (Recommended Security Controls for Federal Information Systems). Los clientes mantienen el control y la responsabilidad de sus datos y de los recursos de medios asociados. Es responsabilidad del cliente administrar los dispositivos móviles de seguridad y el acceso al contenido del cliente.
Seguridad móvil *Aplicaciones aprobadas*	MOS-03	¿Cuenta con una función de cumplimiento de políticas (por ejemplo, XACML) para garantizar que solo las aplicaciones aprobadas y las tiendas que ofrecen dichas aplicaciones se carguen en los dispositivos móviles?	
Seguridad móvil *Software aprobado para BYOD*	MOS-04	¿En su política y capacitación sobre BYOD se especifica claramente cuáles son las aplicaciones y las tiendas de aplicaciones aprobadas para ser usadas en los dispositivos Bring your own device (BYOD, trae tu propio dispositivo)?	

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
Seguridad móvil *Concienciación y capacitación*	MOS-05	¿Cuenta con una política documentada de dispositivos móviles que se proporcione durante la capacitación para empleados y en la que se definan claramente los dispositivos móviles que se pueden usar, el uso aceptado y los requisitos de los dispositivos móviles?	
Seguridad móvil *Servicios basados en la cloud*	MOS-06	¿Cuenta con una lista documentada de servicios basados en la cloud preaprobados que se puedan utilizar para el uso y el almacenamiento de los datos comerciales de la compañía a través de un dispositivo móvil?	
Seguridad móvil *Compatibilidad*	MOS-07	¿Cuenta con un proceso de validación de aplicaciones documentado para probar dispositivos y tratar problemas de compatibilidad de las aplicaciones y los sistemas operativos?	
Seguridad móvil *Elegibilidad de los dispositivos*	MOS-08	¿Cuenta con una política de BYOD en la que se definan los dispositivos y los requisitos de elegibilidad para el uso de BYOD?	
Seguridad móvil *Inventario de dispositivos*	MOS-09	¿Cuenta con un inventario de todos los dispositivos móviles en los que se almacenan datos de la compañía y desde los que se accede a dicha información, incluido el estado de los dispositivos (sistemas operativos y niveles de parches, dispositivos perdidos o fuera de servicio, personas que recibieron los dispositivos)?	
Seguridad móvil *Administración de dispositivos*	MOS-10	¿Cuenta con una solución de administración centralizada de dispositivos móviles implementada en todos los dispositivos móviles que pueden almacenar, transmitir o procesar datos de la compañía?	
Seguridad móvil *Cifrado*	MOS-11	¿En su política sobre dispositivos móviles se exige el uso de cifrado de todo el dispositivo o de los datos identificados como confidenciales mediante los controles de tecnología de todos los dispositivos móviles?	

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
Seguridad móvil *Liberación y enrutamiento*	MOS-12.1	¿En su política sobre dispositivos móviles se prohíbe la elusión de los controles de seguridad incorporados en los dispositivos móviles (por ejemplo, liberación y enrutamiento)?	
	MOS-12.2	¿Cuenta con controles preventivos y de investigación en los dispositivos o a través de un sistema de administración centralizada de dispositivos que prohíba la evasión de controles de seguridad incorporados?	
Seguridad móvil *Aspectos legales*	MOS-13.1	¿En su política sobre BYOD se define claramente la expectativa de privacidad, los requisitos de los litigios, la exhibición de documentos electrónicos y las retenciones legales?	Los clientes mantienen el control y la responsabilidad de sus datos y de los recursos de medios asociados. Es responsabilidad del cliente administrar los dispositivos móviles de seguridad y el acceso al contenido del cliente.
	MOS-13.2	¿Cuenta con controles preventivos y de investigación en los dispositivos o a través de un sistema de administración centralizada de dispositivos que prohíba la evasión de controles de seguridad incorporados?	
Seguridad móvil *Pantalla de bloqueo*	MOS-14	¿Exige el uso de una pantalla de bloqueo automático para los BYOD y los dispositivos que son propiedad de la compañía y regula su implementación a través de controles técnicos?	
Seguridad móvil *Sistemas operativos*	MOS-15	¿Administra todos los cambios de los sistemas operativos de los dispositivos móviles, los niveles de parches y las aplicaciones a través de los procesos de administración de cambios de la compañía?	
Seguridad móvil *Contraseñas*	MOS-16.1	¿Cuenta con políticas de contraseñas para los dispositivos móviles proporcionados por la compañía o los dispositivos móviles BYOD?	
	MOS-16.2	¿Se supervisa el uso de las políticas de contraseñas a través de controles técnicos (por ejemplo, MDM)?	
	MOS-16.3	¿En sus políticas de contraseñas se prohíbe la modificación de los requisitos de autenticación (por ejemplo, longitud de la contraseña o el PIN) a través de un dispositivo móvil?	

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
Seguridad móvil *Políticas*	MOS-17.1	¿Cuenta con una política en la que se exija que los usuarios de BYOD realicen copias de seguridad de los datos corporativos especificados?	
	MOS-17.2	¿Cuenta con una política en la que se prohíba a los usuarios de BYOD usar tiendas de aplicaciones no aprobadas?	
	MOS-17.3	¿Cuenta con una política en la que se exija a los usuarios de BYOD usar software antimalware (en los casos en que corresponda)?	
Seguridad móvil *Borrado remoto*	MOS-18.1	¿Su Departamento de TI proporciona sistemas de borrado remoto o borrado de los datos corporativos para todos los dispositivos BYOD autorizados por la compañía?	
	MOS-18.2	¿Su Departamento de TI proporciona sistemas de borrado remoto o borrado de los datos corporativos para todos los dispositivos móviles asignados por la compañía?	
Seguridad móvil *Parches de seguridad*	MOS-19.1	¿Sus dispositivos móviles cuentan con los parches de seguridad más recientes, instalados luego de la publicación general de parte del fabricante o el proveedor del dispositivo?	
	MOS-19.2	¿En sus dispositivos móviles el personal de TI de la compañía puede realizar la validación remota de las descargas de los últimos parches de seguridad?	
Seguridad móvil *Usuarios*	MOS-20.1	¿En su política de BYOD se especifican los sistemas y servidores que se pueden usar en los dispositivos BYOD autorizados o a los que se puede acceder desde estos?	
	MOS-20.2	En su política de BYOD se especifican los roles de los usuarios que pueden acceder a través de dispositivos BYOD autorizados?	

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
Administración de incidencias de seguridad, exhibición de documentos electrónicos y análisis forense de la cloud *Mantenimiento de contactos y autoridades*	SEF-01.1	¿Mantiene relaciones y puntos de contacto con las autoridades locales en virtud de contratos y de conformidad con los reglamentos apropiados?	AWS mantiene contacto con los organismos del sector, las organizaciones de riesgo y conformidad, las autoridades locales y los organismos normativos de conformidad con el estándar ISO 27001. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
Administración de incidencias de seguridad, exhibición de documentos electrónicos y análisis forense de la cloud *Administración de incidencias*	SEF-02.1	¿Cuenta con un plan documentado para responder a las incidencias de seguridad?	AWS ha implementado un programa y una política formales y documentados de respuesta a incidencias. La política aborda el propósito, el ámbito de aplicación, las funciones, las responsabilidades y el compromiso de la dirección, y se desarrolló de conformidad con los estándares ISO 27001 y NIST 800-53. A continuación se describe el enfoque de tres fases que AWS implementó para administrar las incidencias: 1. Fase de activación y notificación: las incidencias de AWS empiezan con la detección de un evento. Este evento puede proceder de varias fuentes, incluidas: - Métricas y alarmas: AWS es capaz de reconocer las situaciones excepcionales. La mayoría de los problemas se detectan rápidamente con una supervisión las 24 horas del día, los 7 días de la semana, durante los 365 días del año y alarmas procedentes de métricas en tiempo real y paneles de servicios. La mayoría de las incidencias se detectan de esta manera. AWS utiliza alarmas con indicadores tempranos para identificar de forma proactiva los problemas que pueden afectar en última instancia a los clientes. - Vale de problema introducido por un empleado de AWS - Llamadas a la línea telefónica de asistencia técnica, que está disponible las 24 horas del día, los 7 días de la semana, durante los 365 días del año. Si el evento cumple los criterios de incidencia, el ingeniero de soporte de guardia correspondiente iniciará una intervención mediante la herramienta de administración de eventos de AWS para localizar a las personas encargadas de la resolución según el programa (por ejemplo, el equipo de seguridad). Estas personas realizarán un análisis de la incidencia a fin de determinar si es necesario involucrar a más personas y averiguar la raíz aproximada del problema. 2. Fase de recuperación: las personas encargadas de la resolución realizarán soporte técnico reactivo para tratar de abordar la incidencia. Una vez que se ha abordado la solución de problemas, el soporte técnico reactivo y los componentes afectados, el coordinador de la llamada asignará los pasos que hay que seguir a continuación en cuanto a documentación y acciones de seguimiento, y dará por terminada la intervención. 3. Fase de reconstitución: una vez completadas las actividades de corrección pertinentes, el coordinador declarará finalizada la fase de recuperación. Se asignarán al equipo correspondiente el análisis final y un análisis detallado de la causa de la incidencia. La alta dirección examinará los resultados del análisis final y las acciones pertinentes como cambios de diseño, etc. se incluirán en un documento de Correction of Errors (COE, corrección de errores); también se hará un seguimiento de estas hasta su finalización. Además de los mecanismos de comunicación interna explicados anteriormente, AWS también ha implementado varios métodos de comunicación externa para prestar asistencia a su cartera de clientes y a la comunidad. El equipo de atención al cliente dispone de mecanismos para recibir notificaciones sobre problemas operativos que afecten la experiencia de los clientes. El equipo de atención al cliente realiza el mantenimiento del "Panel de estado del servicio" para que se encuentre disponible a fin de advertir al cliente sobre cualquier problema que pueda tener un gran impacto. Los auditores independientes externos revisan el programa de administración de incidencias de AWS durante las auditorías de nuestra conformidad con SOC, PCI DSS, ISO 27001 y FedRAMP. **El documento técnico de seguridad de la cloud de AWS** está disponible en http://aws.amazon.com/security. Allí podrá obtener información adicional.
	SEF-02.2	¿Integra requisitos personalizados para los inquilinos en los planes de respuesta a las incidencias de seguridad?	
	SEF-02.3	¿Publica un documento de funciones y responsabilidades en el que se especifique cuáles son sus funciones y las de sus inquilinos durante las incidencias de seguridad?	
	SEF-02.4	¿Probó sus planes de respuesta ante incidencias de seguridad el año pasado?	
Administración de incidencias de seguridad, exhibición de documentos electrónicos y análisis forense de la cloud *Informes sobre incidencias*	SEF-03.1	¿Combina su sistema de security information and event management (SIEM, administración de eventos e información de seguridad) diversas fuentes de datos (registros de aplicaciones, registros de firewall, registros de ID, registros de accesos físicos, etc.) para poder enviar alertas y realizar análisis detallados?	
	SEF-03.2	¿La estructura de registro y monitoreo permite aislar una incidencia para inquilinos específicos?	

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
Administración de incidencias de seguridad, exhibición de documentos electrónicos y análisis forense de la cloud *Preparación legal de la respuesta a incidencias*	SEF-04.1	¿El plan de respuesta a incidencias cumple las normas del sector en relación con los controles y los procesos de administración de la cadena de custodia admisibles a efectos legales?	
	SEF-04.2	¿La función de respuesta a incidencias incluye la utilización de técnicas de análisis y recopilación de datos forenses admisibles a efectos legales?	
	SEF-04.3	¿Puede respaldar la conservación de documentos debido a litigios (congelación de los datos a partir de un momento dado) de un inquilino concreto sin tener que congelar los datos de otros inquilinos?	
	SEF-04.4	¿Aplica y certifica la separación de los datos de los inquilinos cuando se elabora información para responder a citaciones legales?	
Administración de incidencias de seguridad, exhibición de documentos electrónicos y análisis forense de la cloud *Métricas de respuesta ante incidencias*	SEF-05.1	¿Monitorea y cuantifica el tipo, el volumen y la repercusión de todas las incidencias en la seguridad de la información?	Las métricas de seguridad de AWS se monitorean y analizan de conformidad con el estándar ISO 27001. Consulte la norma ISO 27001, anexo A, dominio 16, para obtener información adicional. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
	SEF-05.2	¿Compartirá datos estadísticos sobre las incidencias en la seguridad de la información con los inquilinos si estos los solicitan?	

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
Responsabilidad, transparencia y administración de la cadena de suministros *Integridad y calidad de los datos*	STA-01.1	¿Revisa y registra los errores en la calidad de los datos y los riesgos asociados, y trabaja junto con sus socios de la cadena de suministros para corregirlos?	Los clientes mantienen el control y la titularidad de la calidad de los datos y de los posibles errores de calidad que podrían surgir como consecuencia del uso de los servicios de AWS. Consulte los informes SOC de AWS para obtener información específica sobre la integridad de datos y la administración de accesos (incluidos los accesos de los usuarios con menos privilegios).
	STA-01.2	¿Diseña e implementa controles para mitigar y contener los riesgos de seguridad de los datos a través de la adecuada separación de tareas, el acceso basado en roles y el acceso menos privilegiado para todo el personal de la cadena de suministros?	
Responsabilidad, transparencia y administración de la cadena de suministros *Generación de informes sobre incidencias*	STA-02.1	¿Proporciona periódicamente la información sobre las incidencias de seguridad a todos los clientes y proveedores afectados a través de métodos electrónicos (por ejemplo, portales)?	El programa, los planes y los procedimientos para responder a las incidencias de AWS se han desarrollado en consonancia con el estándar ISO 27001. En los informes SOC de AWS, se ofrece información acerca de las actividades de control específicas que ejecuta AWS. Consulte el documento técnico de seguridad de la cloud de AWS (disponible en http://aws.amazon.com/security) para obtener información adicional.
Responsabilidad, transparencia y administración de la cadena de suministros *Servicios de infraestructuras y redes*	STA-03.1	¿Recopila datos sobre la capacidad y la utilización de todos los componentes relevantes de la oferta del servicio de la cloud?	AWS administra los datos de capacidad y utilización de conformidad con el estándar ISO 27001. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
	STA-03.2	¿Ofrece a los inquilinos informes sobre la utilización y la planificación de capacidad?	
Responsabilidad, transparencia y administración de la cadena de suministros *Evaluaciones internas de los proveedores*	STA-04.1	¿Realiza evaluaciones internas anuales del cumplimiento y la eficacia de sus políticas, sus procedimientos y las medidas y métricas de respaldo?	El equipo de la cadena de suministro y contratación de AWS mantiene relaciones con todos los proveedores de AWS. Consulte la norma ISO 27001; anexo A, dominio 15, para obtener información adicional. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
Responsabilidad, transparencia y administración de la cadena de suministros *Acuerdos de terceros*	STA-05.1	¿Selecciona y monitorea a los proveedores externos de conformidad con las leyes del país en que se procesan, almacenan y transmiten los datos?	Los requisitos de seguridad del personal de proveedores externos que prestan apoyo a los dispositivos y sistemas de AWS se recogen en un acuerdo mutuo de confidencialidad entre la organización matriz de AWS, Amazon.com, y el proveedor externo correspondiente. El Consejo Jurídico de Amazon y el equipo de contratación de AWS definen los requisitos de seguridad que debe cumplir el personal de los proveedores externos de AWS en acuerdos de contrato con el proveedor externo. Todas las personas que trabajen con información de AWS tienen que superar como mínimo el proceso de cribado previo a la contratación, que consiste en verificar los antecedentes penales, y firmar un Acuerdo de Confidencialidad (NDA) antes de que se les conceda acceso a información de AWS. AWS no suele externalizar el desarrollo de servicios de AWS a subcontratistas.
	STA-05.2	¿Selecciona y monitorea a los proveedores externos de conformidad con las leyes del país en que se originan los datos?	
	STA-05.3	¿El Consejo Jurídico revisa todos los acuerdos de terceros?	
	STA-05.4	¿En los acuerdos de terceros se incluye el aprovisionamiento de seguridad y protección de la información y los recursos?	

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
	STA-05.5	¿Proporciona a los clientes una lista y copias de todos los acuerdos de subprocesamiento y los mantiene actualizados?	
Responsabilidad, transparencia y administración de la cadena de suministros *Revisiones de la gobernanza de la cadena de suministros*	STA-06.1	¿Revisa los procesos de gobernanza y de administración de riesgos de los socios con el objetivo de tener en cuenta los riesgos heredados de otros miembros de dicha cadena de suministros de sus socios?	AWS posee acuerdos formales con los proveedores externos más importantes e implementa los mecanismos de administración de relaciones adecuados, de conformidad con su relación con las diferentes empresas. Los procesos de administración externos de AWS son revisados por auditores independientes como parte del cumplimiento constante de AWS de los informes SOC y el estándar ISO 27001.
Responsabilidad, transparencia y administración de la cadena de suministros *Métricas de la cadena de suministros*	STA-07.1	¿Se establecen políticas y procedimientos, y se respalda la implementación de procesos comerciales y medidas técnicas con el objetivo de cumplir, de forma precisa y absoluta, con los acuerdos relevantes (por ejemplo, SLA) entre los proveedores y los clientes (inquilinos)?	
	STA-07.2	¿Cuenta con la capacidad de medir y abordar problemas de falta de cumplimiento de las disposiciones o los términos a lo largo de toda la cadena de suministros (procesos anteriores y posteriores)?	
	STA-07.3	¿Es capaz de administrar los conflictos en el nivel de servicios o las incoherencias que son consecuencia de las relaciones dispares con los proveedores?	
	STA-07.4	¿Revisa todos los acuerdos, las políticas y los procesos como mínimo una vez por año?	
Responsabilidad, transparencia y administración de la cadena de suministros *Evaluación de terceros*	STA-08.1	¿Garantiza que se cuente con la seguridad razonable de la información en toda la cadena de suministro de información al realizar revisiones anuales?	
	STA-8.2	¿En la revisión anual se incluyen todos los proveedores externos o socios de los que depende su cadena de suministro de información?	
Administración de la cadena de suministros: Transparencia	STA-09.1	¿Permite que los inquilinos ejecuten evaluaciones independientes de las vulnerabilidades?	Los clientes pueden solicitar permiso para realizar análisis de la infraestructura de la cloud siempre que se limiten a las instancias del cliente y no infrinjan la Política de Uso Aceptable de AWS. La aprobación previa para realizar estos tipos de análisis se puede lograr enviando una solicitud a través del Formulario de Solicitud de Pruebas de Intrusión o Vulnerabilidades de AWS.

Grupo de control	CID	Preguntas de Consensus Assessment	Respuesta de AWS
de la cadena de suministros *Auditorías de terceros*	STA-09.2	¿Recurre a algún tercero para que realice análisis de vulnerabilidades y pruebas de intrusión periódicas en las aplicaciones y redes?	AWS Security contrata regularmente a empresas de seguridad independientes para que realicen evaluaciones externas de las amenazas de vulnerabilidades. En los informes SOC de AWS, se ofrecen detalles adicionales acerca de las actividades de control específicas que ejecuta AWS.
Administración de vulnerabilidades y amenazas *Antivirus y software malicioso*	TVM-01.1	¿Tiene programas antimalware instalados en todos los sistemas que admiten o están conectados con las ofertas del servicio de la cloud?	El programa, los procesos y los procedimientos de AWS para administrar el antivirus y el software malicioso están en consonancia con el estándar ISO 27001. Consulte los informes SOC de AWS para obtener información adicional. Además, consulte la norma ISO 27001, anexo A, dominio 12 para obtener más información. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
	TVM-01.2	¿Garantiza que los sistemas de detección de amenazas de seguridad que utilizan firmas, listas o modelos de comportamiento se actualizan en todos los componentes de la infraestructura dentro de los plazos aceptados en el sector?	
Administración de vulnerabilidades y amenazas *Administración de parches y vulnerabilidades*	TVM-02.1	¿Realiza análisis de vulnerabilidades de las capas de red con regularidad como lo prescriben las prácticas recomendadas del sector?	Los clientes mantienen el control de los sistemas operativos invitados, el software y las aplicaciones con los que cuentan, por lo que además son responsables de realizar los análisis de vulnerabilidades y la aplicación de parches a sus propios sistemas. Los clientes pueden solicitar permiso para realizar análisis de la infraestructura de la cloud siempre que se limiten a las instancias del cliente y no infrinjan la Política de Uso Aceptable de AWS. AWS Security analiza con regularidad todas las direcciones IP de punto de enlace de servicio expuestas a Internet a fin de detectar vulnerabilidades. AWS Security notifica al respecto a las partes correspondientes para remediar todas las vulnerabilidades detectadas. La aplicación de parches del sistema y el mantenimiento de AWS no suelen repercutir en los clientes. Consulte el documento técnico de seguridad de la cloud de AWS para obtener información adicional, que se encuentra disponible en http://aws.amazon.com/security. Consulte la norma ISO 27001, anexo A, dominio 12, para obtener información adicional. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
	TVM-02.2	¿Realiza análisis de vulnerabilidades de las capas de las aplicaciones con regularidad de conformidad con regularidad según prescriben las prácticas recomendadas del sector?	
	TVM-02.3	¿Realiza análisis de vulnerabilidades de las capas del sistema operativo local con regularidad según lo prescriben de conformidad con las directrices las prácticas recomendadas del sector?	
	TVM-02.4	¿Facilitará los resultados de los análisis de vulnerabilidades cuando las organizaciones los solicitan?	
	TVM-02.5	¿Puede revisar con rapidez las vulnerabilidades en todos los sistemas, las aplicaciones y los dispositivos informáticos?	
	TVM-02.6	¿Comunicará a los inquilinos los plazos de aplicación de parches de sistemas basados en riesgos si estos los solicitan?	
Administración de vulnerabilidades y amenazas *Código móvil*	TVM-03.1	¿Se autoriza el código móvil antes de su instalación y uso, y se comprueba la configuración del código para garantizar que el código móvil autorizado funciona de conformidad con una política de seguridad claramente definida?	AWS permite a los clientes administrar las aplicaciones cliente y móviles conforme a sus propias necesidades.
	TVM-03.2	¿Se impide la ejecución de todos los códigos móviles no autorizados?	

Apéndice B: Conformidad de AWS con las consideraciones deseguridad de la cloud computing de la Australian Signals Directorate (ASD, Dirección de Señales Australiana)

Las consideraciones de seguridad de la cloud computing se elaboraron para ayudar a las agencias a realizar una evaluación de riesgos de los servicios que ofrecen los proveedores de servicios informáticos en la cloud. A continuación, se explica la conformidad de AWS con las consideraciones de seguridad publicadas en septiembre de 2012. Para obtener más información, visite: http://www.asd.gov.au/publications/csocprotect/Cloud_Computing_Security_Considerations.pdf

Área clave	¿Tiene preguntas?	RESPUESTA DE AWS
Mantenimiento de la disponibilidad y la funcionalidad empresarial	a. Importancia para la empresa de los datos o la funcionalidad. ¿Voy a migrar a la cloud funcionalidad o datos empresariales de vital importancia?	Los clientes de AWS preservan el control y la titularidad de su contenido. Los clientes son responsables de la clasificación y el uso de su contenido.
	b. Plan de recuperación de desastres y continuidad empresarial del proveedor. ¿Puedo estudiar a fondo una copia del plan de recuperación de desastres y continuidad empresarial del proveedor que abarque la disponibilidad y la restauración tanto de mis datos como de los servicios del proveedor que utilizo? ¿Cuánto tiempo se tarda en recuperar mis datos y los servicios que utilizo tras un desastre? ¿Tienen prioridad otros clientes del proveedor que son más grandes y pagan más dinero?	Los clientes de AWS mantienen el control y la propiedad de sus datos. AWS ofrece a los clientes la flexibilidad necesaria para colocar las instancias y almacenar datos en varias regiones geográficas, así como en zonas de disponibilidad múltiples dentro de cada región. Cada zona de disponibilidad está diseñada como una zona de error independiente. En caso de error, los procesos automatizados desvían el tráfico de datos del cliente de la zona afectada. En el informe SOC 1, Tipo 2, de AWS, se ofrece información adicional. En el estándar ISO 27001, Anexo A, dominio 11 se ofrece más información. Un auditor independiente ha validado y certificado AWS a fin de confirmar que está en consonancia con la certificación ISO 27001. Los clientes utilizan AWS para poder realizar una recuperación de desastres más rápida de sus sistemas de TI fundamentales sin incurrir en los gastos adicionales de infraestructuras que supone disponer de un segundo sitio físico. La cloud de AWS presta apoyo a muchas arquitecturas de recuperación de desastres conocidas de entornos de "luz piloto", que están listos para escalar en un momento a entornos de "espera activa" que permiten una rápida conmutación por error. Para obtener más información acerca de la recuperación de desastres en AWS, visite https://aws.amazon.com/disaster-recovery/. AWS ofrece a los clientes la posibilidad de aplicar un sólido plan de continuidad, incluida la utilización de backups frecuentes de las instancias del servidor, replicación de redundancia de los datos y arquitecturas de implementación en varias zonas de disponibilidad y regiones. AWS ofrece a los clientes la flexibilidad necesaria para colocar las instancias y almacenar datos en varias regiones geográficas, así como en zonas de disponibilidad múltiples dentro de cada región. Cada zona de disponibilidad está diseñada como una zona de error independiente. En caso de error, los procesos automatizados desvían el tráfico de datos del cliente de la zona afectada. Los centros de datos de AWS incorporan una protección física frente a riesgos medioambientales. Un auditor independiente ha validado la protección física de AWS frente a riesgos ambientales, que ha certificado su conformidad con las prácticas recomendadas del estándar ISO 27002. Consulte la norma ISO 27001, anexo A, dominio 9, y el informe SOC 1, Tipo II, de AWS para obtener información adicional.

Área clave	¿Tiene preguntas?	RESPUESTA DE AWS
	c. Plan de backup de mis datos. ¿Gastaré más dinero en mantener un backup actualizado de mis datos en las instalaciones de mi agencia o si la almacena un segundo proveedor que no tenga ningún punto de error en común con el primer proveedor?	Los clientes de AWS mantienen el control y la titularidad de su contenido, por lo que tienen la responsabilidad de administrar los planes de backup de sus datos. AWS permite que los clientes extraigan y añadan datos en los servicios de almacenamiento de AWS. El servicio AWS Import/Export para S3 acelera la transferencia de grandes volúmenes de datos desde y hacia AWS utilizando dispositivos de almacenamiento portátiles. AWS permite a los clientes realizar sus propios backups en cintas con su propio proveedor de servicios de backup en cinta. No obstante, AWS no ofrece el servicio de backup en cinta. El servicio de Amazon S3 está diseñado para abordar la probabilidad de que se produzcan pérdidas de datos con un porcentaje próximo a cero, y la durabilidad equivalente de copias en varios sitios de los objetos de datos se consigue con la redundancia del almacenamiento de los datos. Para obtener información acerca de la redundancia y la durabilidad de los datos, consulte el sitio web de AWS. AWS ofrece una gama completa de servicios de cloud computing para la recuperación de desastres. Para obtener más información acerca de la recuperación de desastres en AWS, visite https://aws.amazon.com/disaster-recovery/.
	d. Mi plan de recuperación de desastres y continuidad empresarial. ¿Gastaré más dinero en replicar mis datos o la funcionalidad empresarial con un segundo proveedor que utilice un centro de datos diferente e idealmente no tenga ningún punto de error en común con el primer proveedor? Esta replicación debe configurarse preferiblemente para que se realice de forma automática una "conmutación por error", de modo que si los servicios de un proveedor dejan de estar disponibles, el control pase al otro proveedor automáticamente y sin interrupciones.	Los clientes mantienen el control y la propiedad de sus datos. Los clientes pueden exportar sus AMI y utilizarlas en las instalaciones o con otro proveedor (sujetos a restricciones de licencias de software). Consulte el documento técnico de información general sobre los procesos de seguridad de AWS para obtener más información, que se encuentra disponible en http://aws.amazon.com/security. AWS permite que los clientes extraigan y añadan datos en los servicios de almacenamiento de AWS. El servicio AWS Import/Export para S3 acelera la transferencia de grandes volúmenes de datos desde y hacia AWS utilizando dispositivos de almacenamiento portátiles. AWS permite a los clientes realizar sus propios backups en cintas con su propio proveedor de servicios de backup en cinta. No obstante, AWS no ofrece el servicio de backup en cinta. Los centros de datos de AWS están agrupados en clústeres en varias regiones del mundo. Todos los centros de datos están online y a disposición de los clientes, por lo que ninguno está "inactivo". En caso de error, los procesos automatizados desvían el tráfico de datos del cliente de la zona afectada. Las aplicaciones principales se implementan en una configuración N+1, de forma que en el caso de que se produzca un error en el centro de datos, haya capacidad suficiente para permitir equilibrar la carga del tráfico entre los demás sitios. AWS ofrece a los clientes la flexibilidad necesaria para colocar las instancias y almacenar datos en varias regiones geográficas, así como en zonas de disponibilidad múltiples dentro de cada región. Cada zona de disponibilidad está diseñada como una zona de error independiente. Esto significa que las zonas de disponibilidad están físicamente separadas dentro de una región metropolitana habitual y se encuentran en llanuras poco propensas a inundaciones (las categorías específicas de zonas propensas a inundaciones varían según la región). Además de las instalaciones de sistemas de alimentación ininterrumpida (SAI) discretos y de generación de copias de seguridad in situ, se alimentan a través de diferentes redes a partir de utilidades independientes para reducir aún más cada uno de los puntos de error. Todas las zonas de disponibilidad están conectadas de forma redundante a varios proveedores de tránsito de nivel 1. Los clientes deben planificar el uso que realizan de AWS para poder utilizar varias regiones y zonas de disponibilidad. La distribución de aplicaciones por varias zonas de disponibilidad ofrece la posibilidad de mantener la resistencia ante la mayoría de los modos de error, incluidos los desastres naturales o los errores del sistema. En el informe SOC 1, Tipo 2, de AWS, se ofrece información adicional. En el estándar ISO 27001, Anexo A, dominio 11 se ofrece más información. Un auditor independiente ha validado y certificado AWS a fin de confirmar que está en consonancia con la certificación ISO 27001.

Área clave	¿Tiene preguntas?	RESPUESTA DE AWS
	e. Mi conectividad de red con la cloud. ¿La conectividad de red entre los usuarios de mi agencia y la red del proveedor es adecuada en cuanto a disponibilidad, rendimiento del tráfico (ancho de banda), retrasos (latencia) y pérdida de paquetes?	Los clientes también pueden elegir su ruta de acceso de red a las instalaciones de AWS, incluidos varios puntos de enlace de VPN en cada región de AWS. Además, AWS Direct Connect facilita el establecimiento de una conexión de red dedicada entre sus instalaciones y AWS. Con AWS Direct Connect, puede establecer conectividad privada entre AWS y su centro de datos, oficina o entorno de coubicación, lo que en muchos casos puede reducir los costos de red, aumentar el rendimiento del ancho de banda y proporcionar una experiencia de red más constante que las conexiones basadas en Internet. Consulte el documento técnico de información general sobre los procesos de seguridad de AWS para obtener más información, que se encuentra disponible en http://aws.amazon.com/security.
	f. Garantía de disponibilidad del proveedor. ¿El Acuerdo de nivel de servicios (SLA) garantiza que el proveedor ofrecerá una disponibilidad de sistema y una calidad de servicio adecuadas con sus procesos empresariales y su arquitectura del sistema sólidos?	AWS confirma altos niveles de disponibilidad en sus acuerdos de nivel de servicios (SLA). Por ejemplo, Amazon EC2 garantiza un porcentaje anual de tiempo de actividad de al menos el 99,95 % durante el año de servicio. Amazon S3 garantiza un porcentaje de tiempo de actividad mensual de al menos el 99,99 %. Se ofrecen créditos de servicio para los casos en que no se cumplan estas métricas de disponibilidad. Los clientes deben planificar el uso que realizan de AWS para poder utilizar varias regiones y zonas de disponibilidad. La distribución de aplicaciones por varias zonas de disponibilidad ofrece la posibilidad de mantener la resistencia ante la mayoría de los modos de error, incluidos los desastres naturales o los errores del sistema. AWS utiliza sistemas automáticos de monitoreo para ofrecer un alto nivel de rendimiento y disponibilidad de los servicios. El monitoreo proactivo se encuentra disponible a través de una serie de herramientas en línea destinadas tanto para uso interno como externo. Los sistemas de AWS disponen de una gran variedad de recursos para poder monitorear las principales métricas operativas. Las alarmas se configuran para notificar al personal de operaciones y administración cuándo las métricas operativas clave superan los umbrales de advertencias anticipadas. Se utiliza un programa de asistencia de guardia a fin de que este personal esté siempre disponible para solucionar los problemas de funcionamiento. Incluye además un sistema de localización de personas para que las alarmas se comuniquen al personal de operaciones de forma rápida y fiable. Los auditores independientes externos revisan periódicamente la administración de la red de AWS como parte de nuestro programa continuado de conformidad con SOC, PCI DSS, ISO 27001 y FedRAMP[sm].
	g. Impacto de las interrupciones del servicio. ¿Puedo tolerar el máximo tiempo de inactividad posible del SLA? ¿Los períodos de interrupción programados son aceptables tanto en duración como en lo que respecta a la hora del día o las interrupciones programadas interferirán con mis procesos empresariales esenciales?	AWS no necesita interrumpir los sistemas para realizar tareas regulares de mantenimiento ni para aplicar parches a los mismos. La aplicación de parches del sistema y el mantenimiento de AWS no suelen repercutir en los clientes. El cliente es el encargado de controlar el mantenimiento de las instancias.

Área clave	¿Tiene preguntas?	RESPUESTA DE AWS
	h. Inclusión en el SLA de las interrupciones programadas. ¿El porcentaje de disponibilidad garantizado por el SLA incluye las interrupciones programadas?	AWS no administra ningún entorno con interrupciones programadas, ya que ofrece a los clientes la posibilidad de que diseñen sus entornos para aprovechar la existencia de diversas regiones y zonas de disponibilidad.
	i. Compensación contemplada en el SLA. ¿El SLA refleja adecuadamente los daños reales ocasionados por el incumplimiento del SLA, como pueden ser tiempos de inactividad no programados o pérdidas de datos?	AWS indemniza a los clientes por las pérdidas que puedan sufrir debido a las interrupciones de los servicios de conformidad con el Acuerdo de Nivel de Servicios de AWS.
	j. Disponibilidad e integridad de los datos. ¿Cómo implementa el proveedor mecanismos como la redundancia y las copias de seguridad remotas para impedir daños o pérdidas de mis datos y garantizar la integridad y la disponibilidad de dichos datos?	Los controles de integridad de los datos de AWS, tal y como se describen en el informe SOC 1, Tipo II, de AWS, ofrecen garantías razonables de que se mantiene la integridad de los datos en todas las fases, entre otras, la transmisión, el almacenamiento y el procesamiento. Además, consulte la norma ISO 27001, anexo A, dominio 12, para obtener información adicional. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001. Los centros de datos están agrupados en varias regiones del mundo. AWS ofrece a los clientes la flexibilidad necesaria para colocar las instancias y almacenar datos en varias regiones geográficas, así como en zonas de disponibilidad múltiples dentro de cada región. Los clientes deben planificar el uso que realizan de AWS para poder utilizar varias regiones y zonas de disponibilidad. Usted elige dónde se almacenan sus datos al especificar una región (en el caso de Amazon S3) o una zona de disponibilidad de una región (para EBS). Los datos almacenados en volúmenes de Amazon Elastic Block Store (EBS) se almacenan de forma redundante en varias ubicaciones físicas como parte del funcionamiento normal de dichos servicios y sin cargo adicional. No obstante, la replicación de Amazon EBS se almacena en la misma zona de disponibilidad, no en varias zonas. Amazon S3 ofrece una infraestructura de almacenamiento que presenta elevados niveles de durabilidad. Los objetos se almacenan de forma redundante en varios dispositivos de diversas instalaciones dentro de una región de Amazon S3. Una vez almacenados, Amazon S3 mantiene la durabilidad de los objetos detectando y reparando rápidamente cualquier pérdida de redundancia. Del mismo modo, Amazon S3 comprueba de forma regular la integridad de los datos almacenados mediante sumas de comprobación. Si se detecta algún tipo de daño en los objetos, se reparan utilizando los datos redundantes. En caso de los datos almacenados en S3, el servicio está diseñado para ofrecer una durabilidad del 99,999999999 % y una disponibilidad de los objetos del 99,99 % durante un año concreto. Consulte el documento técnico de información general sobre los procesos de seguridad de AWS para obtener más información, que se encuentra disponible en http://aws.amazon.com/security.

Área clave	¿Tiene preguntas?	RESPUESTA DE AWS
	k. Restauración de los datos. Si elimino accidentalmente un archivo, un mensaje de correo electrónico u otros datos, ¿cuánto tiempo se tarda en restaurar mis datos parcial o totalmente a partir de un backup? ¿El tiempo máximo aceptable se especificó en el SLA?	Los clientes de AWS mantienen el control y la propiedad de sus datos. AWS ofrece a los clientes la flexibilidad necesaria para colocar las instancias y almacenar datos en varias regiones geográficas, así como en zonas de disponibilidad múltiples dentro de cada región.
	l. Escalabilidad. ¿Cuántos recursos informáticos de reserva me ofrece el proveedor para que pueda escalar sus servicios con poca antelación?	La cloud de AWS está distribuida y es muy segura y resistente, por lo que ofrece a los clientes un gran potencial de escalado. Los clientes pueden aumentar o reducir el escalado y pagar solo por lo que utilicen.
	m. Cambio de proveedor. Si quiero llevar mis datos a mi agencia o a otro proveedor, o si el proveedor quiebra o abandona el negocio de la cloud repentinamente, ¿cómo accedo a mis datos en un formato independiente del proveedor para evitar depender de él? ¿En qué medida cooperará el proveedor? ¿Cómo me aseguro de que mis datos se eliminen de forma permanente de los medios de almacenamiento del proveedor? En el caso de plataforma como servicio, ¿qué normas utiliza el proveedor que faciliten la portabilidad y la interoperabilidad para trasladar fácilmente mi aplicación a otro proveedor o a mi agencia?	Los clientes mantienen el control y la propiedad de sus datos. Los clientes pueden exportar sus AMI y utilizarlas en las instalaciones o con otro proveedor (sujetos a restricciones de licencias de software). Consulte el documento técnico de información general sobre los procesos de seguridad de AWS para obtener más información, que se encuentra disponible en http://aws.amazon.com/security. AWS permite que los clientes extraigan y añadan datos en los servicios de almacenamiento de AWS. El servicio AWS Import/Export para S3 acelera la transferencia de grandes volúmenes de datos desde y hacia AWS utilizando dispositivos de almacenamiento portátiles. AWS permite a los clientes realizar sus propios backups en cintas con su propio proveedor de servicios de backup en cinta. No obstante, AWS no ofrece el servicio de backup en cinta.

Área clave	¿Tiene preguntas?	RESPUESTA DE AWS
Protección de los datos frente al acceso no autorizado de un tercero	a. Elección del modelo de implementación de la cloud. ¿Puedo contemplar la posibilidad de utilizar una cloud pública que es posiblemente menos segura, una cloud híbrida o de la comunidad que es posiblemente más segura, o una cloud privada, que es la más segura?	Los equipos de conformidad y seguridad de AWS han creado una estructura de seguridad de la información y políticas relacionadas basadas en la estructura de los Control Objectives for Information and related Technology (COBIT, Objetivos de control para información y tecnologías relacionadas). La estructura de seguridad de AWS integra las prácticas recomendadas de la ISO 27002 y el estándar de seguridad de los datos de PCI. Consulte el documento técnico Riesgos y conformidad de AWS para obtener más detalles. Este está disponible en http://aws.amazon.com/security. AWS facilita directamente a nuestros clientes, de conformidad con acuerdos de nivel de servicios, acreditaciones independientes, certificaciones, el informe Service Organization Controls 1 (SOC 1), Tipo II, y otros informes de conformidad relevantes. Amazon Virtual Private Cloud (Amazon VPC) le permite aprovisionar una sección aislada de forma lógica de la cloud de Amazon Web Services (AWS), donde puede lanzar recursos de AWS en una red virtual que usted defina. Puede controlar todos los aspectos del entorno de red virtual, incluida la selección de su propio rango de direcciones IP, la creación de subredes y la configuración de tablas de enrutamiento y puertas de enlace de red. Es fácil personalizar la configuración de red de Amazon VPC. Por ejemplo, puede crear una subred de cara al público para los servidores web con acceso a Internet y colocar los sistemas de fondo, como bases de datos o servidores de aplicaciones, en una subred de uso privado sin acceso a Internet. Puede aprovechar varias capas de seguridad, incluidos grupos de seguridad y listas de control de acceso a red, para ayudar a controlar el acceso a las instancias de Amazon EC2 desde cada subred. Además, también puede crear una conexión de red privada virtual (VPN) de hardware entre el centro de datos corporativo y su VPC, y aprovechar la cloud de AWS como una ampliación del centro de datos corporativo.
	b. Confidencialidad de mis datos. ¿Los datos que se almacenarán o procesarán en la cloud se consideran información reservada, confidencial y privada; o información que está disponible para todo el público, al igual que la información de mi sitio web público? ¿La agregación de mis datos los hace más confidenciales que cualquier dato individual? Por ejemplo, la confidencialidad puede aumentar si almaceno una gran cantidad de datos o si almaceno diferentes datos que, en su conjunto, facilitarían el robo de identidad. Si se ponen en peligro los datos, ¿podría demostrar mi diligencia debida a la alta dirección, los funcionarios gubernamentales y el público?	Los clientes de AWS mantienen el control y la titularidad de sus datos y pueden aplicar un programa de clasificación de datos estructurado para satisfacer sus necesidades.

Área clave	¿Tiene preguntas?	RESPUESTA DE AWS
	c. Obligaciones legales. ¿Con qué obligaciones cuento para proteger y administrar mis datos de conformidad con las diferentes legislaciones; por ejemplo, la Ley de Privacidad, la Ley de Archivos u otras leyes específicas según el tipo de datos? ¿El proveedor aceptará por contrato la adhesión a estas obligaciones para ayudarme a garantizar que se cumplen esas obligaciones a satisfacción del gobierno australiano?	Los clientes de AWS tienen la responsabilidad de garantizar que el uso que hacen de AWS cumpla con los reglamentos y las leyes aplicables. AWS informa acerca de su entorno de control y seguridad a los clientes a través de acreditaciones independientes y certificaciones del sector y documentos técnicos (disponibles en http://aws.amazon.com/security), además de ofrecer certificaciones, informes y otra documentación relevante directamente a los clientes de AWS. AWS ha publicado un documento técnico sobre el uso de AWS en el contexto de las consideraciones sobre la privacidad australianas, que está disponible aquí.
	d. Países con acceso a mis datos. ¿En qué países se almacenan, procesan y se hacen copias de seguridad de mis datos? ¿Por cuáles países extranjeros se trasmiten mis datos? ¿En qué países se realiza la conmutación por error o están los centros de datos redundantes? ¿El proveedor me notificará si cambian las respuestas a estas preguntas?	Los clientes de AWS eligen la región o regiones de AWS donde se ubicarán el contenido y los servidores. De esta forma, los clientes que tengan requisitos geográficos específicos pueden establecer entornos en las ubicaciones que deseen. Los clientes de AWS en Australia pueden elegir implementar sus servicios de AWS solamente en la región Asia Pacífico (Sídney) y almacenar su contenido en Australia. Si el cliente elige esta opción, su contenido se ubicará en Australia, a menos que decida trasladar los datos. Los clientes pueden replicar y hacer copias de seguridad del contenido en más de una región, pero AWS no mueve ni replica el contenido fuera de la región o las regiones elegidas por el cliente. AWS vela por la seguridad de los clientes y no divulga ni mueve datos como respuesta a una solicitud del gobierno australiano, estadounidense o de otro país, a menos que sea necesario para cumplir con una orden válida legalmente y vinculante, como una citación o una orden judicial, o cuando así lo exijan las leyes aplicables. Los organismos gubernamentales o reguladores de otros países distintos de EE. UU. deben utilizar normalmente procesos internacionales reconocidos, como los tratados de asistencia judicial recíproca con el gobierno de EE. UU., para obtener órdenes válidas y vinculantes. Además, nuestra práctica consiste en notificar a los clientes antes de divulgar su contenido, cuando ello sea posible, para que tengan la oportunidad de buscar amparo frente a la divulgación de la información, salvo que haya alguna incompatibilidad legal.

Área clave	¿Tiene preguntas?	RESPUESTA DE AWS
	e. Tecnologías de cifrado de datos. ¿El ISM de DSD utilizado para proteger mis datos, tanto cuando están en tránsito a través de una red como cuando se almacenan en los equipos y los medios de backup del proveedor, considera adecuadas las longitudes de clave, los algoritmos hash y los algoritmos de cifrado? La posibilidad de cifrar datos mientras se están procesando en los equipos del proveedor es todavía una tecnología emergente y está en estudio en el sector y en los círculos académicos. ¿Se considera que el cifrado es lo suficientemente seguro como para proteger mis datos mientras estos sean confidenciales?	AWS permite a los clientes utilizar sus propios mecanismos de cifrado prácticamente para todos los servicios, entre otros, S3, EBS, SimpleDB y EC2. También se cifran las sesiones de VPC. Amazon S3 también ofrece a los clientes la opción de utilizar el cifrado del servidor. Además, los clientes también pueden utilizar tecnologías de cifrado de terceros. Internamente, AWS establece y administra claves de cifrado para la criptografía necesaria empleada en la infraestructura de AWS. AWS produce, controla y distribuye claves criptográficas simétricas mediante los procesos y la tecnología de administración de claves del sistema de información de AWS aprobados por el NIST. Se utiliza un administrador de credenciales y claves seguras desarrollado por AWS para crear, proteger y distribuir claves simétricas, así como para proteger y distribuir: credenciales de AWS necesarias en los hosts, claves públicas y privadas de RSA y certificaciones X.509. Los auditores independientes externos revisan los procesos de cifrado de AWS como parte de nuestro programa continuado de conformidad con SOC, PCI DSS, ISO 27001 y FedRAMP[sm]. El servicio AWS CloudHSM le permite proteger sus claves de encriptado dentro de los dispositivos HSM diseñados y aprobados de acuerdo con los estándares gubernamentales para la administración segura de claves. Puede crear, almacenar y administrar de manera segura las claves utilizadas para el encriptado de datos, de modo que solo sean accesibles para usted. AWS CloudHSM lo ayuda a cumplir con los estrictos requisitos para la administración de claves sin reducir el rendimiento de la aplicación. El servicio AWS CloudHSM funciona con Amazon Virtual Private Cloud (VPC). Los dispositivos CloudHSM se suministran en su VPC con la dirección IP que usted especifique, lo que proporciona una conectividad de red sencilla y privada a sus instancias de Amazon Elastic Compute Cloud (EC2). La ubicación de dispositivos CloudHSM cerca de sus instancias de EC2 reduce la latencia de la red, lo cual mejora el rendimiento de la aplicación. AWS proporciona acceso dedicado y exclusivo a los dispositivos CloudHSM, no disponible para otros clientes de AWS. Disponible en varias regiones y zonas de disponibilidad, AWS CloudHSM le permite añadir un almacenamiento para claves seguro y duradero a sus aplicaciones de Amazon EC2
	f. Saneamiento de soportes. ¿Qué procesos se utilizan para sanear los soportes en los que se almacenan mis datos al final de su vida útil? ¿El ISM de DSD considera adecuados estos procesos?	Cuando un dispositivo de almacenamiento alcanza el final de su vida útil, los procedimientos de AWS incluyen un proceso de retirada diseñado para prevenir que los datos de los clientes queden expuestos al acceso de personas no autorizadas. AWS utiliza las técnicas detalladas en DoD 5220.22-M ("Manual de operaciones del programa de seguridad industrial nacional") o NIST 800-88 ("Directrices para el saneamiento de soportes") para destruir datos como parte del proceso de retirada. En caso de que no se pueda retirar un dispositivo de hardware con estos procedimientos, el dispositivo se desmagnetizará o destruirá físicamente de conformidad con las prácticas estándar del sector. Consulte el documento técnico de información general sobre los procesos de seguridad de AWS para obtener más información, que se encuentra disponible en http://aws.amazon.com/security.

Área clave	¿Tiene preguntas?	RESPUESTA DE AWS
	g. Monitoreo y administración remotos del proveedor. ¿El proveedor monitorea o administra los equipos en los que se almacenan o procesan mis datos? En caso afirmativo, ¿esto se realiza de forma remota desde otros países extranjeros o desde Australia? ¿El proveedor puede proporcionar informes de conformidad de parches y otros detalles relativos a la seguridad de las estaciones de trabajo utilizadas para realizar este trabajo? ¿Qué controles impiden que los empleados del proveedor utilicen de manera no fiable sus portátiles personales?	Al migrar la infraestructura de TI a los servicios de AWS, se crea un modelo de responsabilidad compartida entre el cliente y AWS. Este modelo compartido puede aliviar la carga operativa del cliente, ya que AWS opera, administra y controla los componentes del sistema operativo host y la capa de virtualización, a fin de ofrecer seguridad física en las instalaciones en las que operan los servicios. Por otra parte, el cliente asume la responsabilidad y la administración del sistema operativo invitado (incluidas las actualizaciones y los parches de seguridad) de cualquier otro software de aplicaciones asociadas y de la configuración del firewall del grupo de seguridad que ofrece AWS.
	h. Mi monitoreo y administración. ¿Puedo utilizar mis herramientas actuales para comprobar la integridad y la conformidad, monitorear la seguridad y administrar la red para tener mejor visibilidad de todos mis sistemas, independientemente de si son locales o si están ubicados en la cloud? ¿Tengo que aprender a utilizar herramientas adicionales que proporcione el proveedor? ¿El proveedor me ofrece algún mecanismo para que yo realice el monitoreo?	AWS CloudWatch proporciona el monitoreo de los recursos de la cloud de AWS y de las aplicaciones que los clientes ejecutan en AWS. Consulte aws.amazon.com/cloudwatch para obtener información adicional. AWS también publica la información más actualizada sobre la disponibilidad del servicio en el Panel de estado del servicio. Visite status.aws.amazon.com. AWS Trusted Advisor inspecciona el entorno de AWS y realiza recomendaciones cuando surge la oportunidad de ahorrar dinero, mejorar el rendimiento del sistema y la fiabilidad o ayudar a solucionar errores de seguridad.
	i. Titularidad de los datos. ¿Conservo la titularidad legal de mis datos o pertenece al proveedor y los liquidadores pueden considerarlos un recurso disponible para la venta si el proveedor se declara en quiebra?	Los clientes de AWS mantienen el control y la propiedad de sus datos. AWS solo utiliza el contenido de cada cliente para proporcionar los servicios de AWS seleccionados por cada cliente a dicho cliente y no utiliza el contenido de los clientes para ningún propósito secundario. AWS trata del mismo modo todo el contenido de los clientes y no sabe el tipo de contenido que estos deciden almacenar en AWS. AWS se limita a poner a disposición del cliente los servicios de informática, almacenamiento, base de datos y red elegidos por él. AWS no necesita acceder al contenido de ningún cliente para proporcionarle los servicios.

Área clave	¿Tiene preguntas?	RESPUESTA DE AWS
	j. Tecnologías de puerta de enlace. ¿Qué tecnologías utiliza el proveedor para crear un entorno de puerta de enlace seguro? Por ejemplo, firewalls, filtros del flujo de tráfico, filtros de contenido y software antivirus y diodos de datos según corresponda.	La red de AWS ofrece protección de alto nivel frente a los problemas tradicionales de seguridad de la red y los clientes pueden implementar medidas adicionales de protección. Consulte el documento técnico de información general sobre los procesos de seguridad de AWS para obtener más información, que se encuentra disponible en http://aws.amazon.com/security. Los recursos de Amazon (por ejemplo, los dispositivos portátiles) están configurados con software antivirus que incluye filtrado de correo electrónico y detección de malware. Los auditores independientes externos revisan la administración de los firewalls de red de AWS y el programa antivirus de Amazon como parte de nuestro programa continuado de conformidad con SOC, PCI DSS, ISO 27001 y FedRAMP[sm].
	k. Certificación de la puerta de enlace. ¿El entorno de puerta de enlace del proveedor está certificado conforme a los estándares y las regulaciones sobre seguridad del gobierno?	AWS obtiene ciertas certificaciones del sector y acreditaciones independientes, entre las que se incluye el entorno de puerta de enlace de AWS.
	l. Filtrado de contenido de correo electrónico. En el caso de software de correo electrónico como servicio, ¿el proveedor ofrece filtrado de contenido de correo electrónico personalizable que pueda aplicar la política de contenido de correo electrónico de mi agencia?	Un cliente puede utilizar un sistema para alojar capacidades de correo electrónico; sin embargo, en ese caso el cliente es responsable de emplear los niveles adecuados de protección contra spam y malware en los puntos de entrada y salida de correo electrónico, así como de actualizar las definiciones de spam y malware cuando haya nuevas versiones disponibles.

Área clave	¿Tiene preguntas?	RESPUESTA DE AWS
	m. Políticas y procesos que apoyan el nivel de seguridad de TI del proveedor. ¿Puedo obtener detalles de cómo el nivel de seguridad de la red y de los equipos del proveedor está respaldado por políticas y procesos, incluidas evaluaciones de amenazas y riesgos, administración continua de vulnerabilidades, un proceso de administración de cambios que incorpore seguridad, pruebas de intrusión, registro y análisis periódico de logs, uso de productos de seguridad respaldados por el gobierno australiano, y conformidad con los estándares y las regulaciones sobre seguridad del gobierno australiano?	El departamento de seguridad de la información de AWS ha establecido políticas y procedimientos basados en la estructura de COBIT, los estándares de la ISO 27001 y las disposiciones de PCI DSS. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001. Además, AWS publica un informe SOC 1, Tipo II. Consulte el informe SOC 1 para obtener información adicional. Consulte el documento técnico sobre riesgos y conformidad de AWS para obtener información adicional, que se encuentra disponible en http://aws.amazon.com/security. Los clientes de AWS pueden identificar los principales controles administrados por AWS. Los controles principales son de vital importancia para el entorno de control del cliente y se precisa de una acreditación externa sobre la eficacia operativa de estos controles con el fin de satisfacer los requisitos de conformidad, como la auditoría financiera anual. Para tal fin, AWS publica un amplio abanico de controles de TI específicos en su informe Service Organization Controls 1 (SOC 1), Tipo II. El informe SOC 1, denominado anteriormente Declaración de Estándares de Auditoría (SAS) Nº 70, Organizaciones de Servicios, y conocido antiguamente como Statement on Standards for Attestation Engagements Nº 16 (SSAE 16), es un estándar de auditoría reconocido ampliamente que desarrolla el American Institute of Certified Public Accountants (AICPA). La auditoría SOC 1 es una auditoría exhaustiva utilizada para evaluar el diseño y la eficacia operativa de los objetivos y las actividades de control de AWS, entre otros, aquellos que comprenden parte de la infraestructura que AWS administra. La categoría "Tipo II" hace referencia al hecho de que cada uno de los controles descritos en el informe no solo se evalúa en términos de idoneidad del diseño, sino que los auditores externos también comprueban su eficacia operativa. Habida cuenta de la independencia y las competencias del auditor externo de AWS, los controles identificados en el informe aportan a los clientes un alto nivel de confianza en el entorno de control de AWS.
	n. Tecnologías que apoyan el nivel de seguridad de TI del proveedor. ¿Puedo obtener detalles de cómo el nivel de seguridad de la red y de los equipos del proveedor está respaldado por controles técnicos directos, incluida la aplicación puntual de parches de seguridad, software antivirus que se actualiza periódicamente, mecanismos de defensa en profundidad para protegerse frente a vulnerabilidades desconocidas, sistemas operativos reforzados y aplicaciones de software configuradas con los parámetros de seguridad más estrictos posible, sistemas de prevención y detección de intrusiones, y mecanismos de prevención de pérdida de datos?	AWS facilita directamente a nuestros clientes, de conformidad con acuerdos de nivel de servicios, acreditaciones independientes, certificaciones, el informe Service Organization Controls 1 (SOC 1), Tipo II, y otros informes de conformidad relevantes. AWS Security analiza con regularidad todas las direcciones IP de punto de enlace de los servicios expuestas a Internet a fin de detectar vulnerabilidades (estos análisis no incluyen las instancias de los clientes). AWS Security notifica al respecto a las partes correspondientes para remediar todas las vulnerabilidades detectadas. Asimismo, empresas de seguridad independientes realizan con regularidad evaluaciones de amenazas de vulnerabilidades externas. Los resultados y las recomendaciones derivados de estas evaluaciones se clasifican y, además, se entregan a los equipos directivos de AWS. Asimismo, el entorno de control de AWS está sujeto a evaluaciones de riesgos internas y externas de carácter regular. AWS colabora con auditores independientes y organismos de certificación externos para revisar y probar el entorno de control global de AWS.

Área clave	¿Tiene preguntas?	RESPUESTA DE AWS
	o. Auditoría del nivel de seguridad de TI del proveedor. ¿Puedo auditar la implementación que hace el proveedor de las medidas de seguridad, incluida la realización de escaneos y otras pruebas de intrusión del entorno que se me proporciona? Si existe alguna razón justificable por la cual no es posible realizar la auditoría, ¿qué tercero acreditado ha realizado auditorías y otras evaluaciones de vulnerabilidades? ¿Qué tipo de auditorías internas realiza el proveedor, y qué estándares de conformidad y otras prácticas recomendadas de organizaciones como la Cloud Security Alliance se utilizan para estas evaluaciones? ¿Puedo examinar minuciosamente una copia de los informes de resultados recientes?	AWS facilita directamente a nuestros clientes, de conformidad con acuerdos de nivel de servicios, acreditaciones independientes, certificaciones, el informe Service Organization Controls 1 (SOC 1), Tipo II, y otros informes de conformidad relevantes. Los clientes pueden solicitar permiso para realizar análisis de la infraestructura de la cloud siempre que se limiten a las instancias del cliente y no infrinjan la Política de uso aceptable de AWS. La aprobación previa para realizar estos tipos de análisis se puede obtener enviando una solicitud a través del Formulario de Solicitud de Pruebas de Intrusión o Vulnerabilidades de AWS. AWS Security contrata regularmente a empresas de seguridad independientes para que realicen evaluaciones externas de las amenazas de vulnerabilidades. En el informe SOC 1, Tipo 2, de AWS, se ofrecen detalles adicionales acerca de las actividades de control específicas que ejecuta AWS.

Área clave	¿Tiene preguntas?	RESPUESTA DE AWS
	p. Autenticación de los usuarios. ¿Qué sistemas de administración de acceso e identidades admite el proveedor para el inicio de sesión de los usuarios a fin de utilizar el modelo de software como servicio?	AWS Identity and Access Management (IAM) permite controlar de forma segura el acceso a servicios y recursos de AWS por parte de sus usuarios. Con IAM puede crear y administrar usuarios y grupos de AWS, así como utilizar permisos para permitir o denegar el acceso a los recursos de AWS. AWS admite la federación de identidades, que simplifica la administración de usuarios al mantener sus identidades en un único lugar. AWS IAM incluye compatibilidad con el lenguaje de marcado para confirmaciones de seguridad (SAML, Security Assertion Markup Language) 2.0, un estándar abierto que utilizan muchos proveedores de identidades. Esta nueva característica permite el inicio de sesión único federado, o SSO, y permite a los usuarios iniciar sesión en AWS Management Console o realizar llamadas mediante programación a las API de AWS, mediante aserciones de un proveedor de identidades compatible con SAML, como Shibboleth y Servicios de federación de Active Directory de Windows.
	q. Control centralizado de los datos. ¿Qué formación para los usuarios, políticas y controles técnicos impiden que los usuarios de mi agencia empleen dispositivos informáticos no aprobados o inseguros sin un entorno operativo de confianza para almacenar o procesar datos confidenciales a los que se accede mediante una plataforma de software como servicio?	N/D

Área clave	¿Tiene preguntas?	RESPUESTA DE AWS
	r. Nivel de seguridad física del proveedor. ¿El proveedor utiliza productos y dispositivos físicos de seguridad respaldados por el gobierno australiano? ¿Cómo está diseñado el centro de datos físico del proveedor para impedir la manipulación o el robo de servidores, infraestructura y los datos almacenados en ellos? ¿El centro de datos físico del proveedor está acreditado por un tercero autorizado?	La definición de los controles lógicos y físicos definidos por AWS está documentada en el informe SOC 1, Tipo II, y el informe se encuentra disponible para que los equipos de auditoría y conformidad puedan revisarlo. La certificación ISO 27001 y otras certificaciones de AWS también se encuentran disponibles para su revisión por parte de los auditores. Los controles de seguridad física incluyen, pero no se limitan a, controles perimetrales como vallas, muros, personal de seguridad, videovigilancia, sistemas de detección de intrusiones y otros medios electrónicos. El acceso físico está estrictamente controlado tanto en el perímetro como en los puntos de acceso del edificio e incluye, entre otros aspectos, personal de seguridad profesional mediante videovigilancia, sistema de detección de intrusiones y otros recursos electrónicos. El personal autorizado debe confirmar una autenticación de dos factores como mínimo dos veces para acceder a los pisos del centro de datos. Los puntos de acceso físico a las ubicaciones de los servidores se graban con cámaras de televisión de circuito cerrado (closed circuit television camera, CCTV), tal y como se define en la política de seguridad física del centro de datos de AWS. Las imágenes se conservan durante 90 días, a menos que este período esté limitado a 30 en virtud de las disposiciones legales o contractuales AWS ofrece acceso físico al centro de datos y facilita información a los empleados y contratistas aprobados que tengan una necesidad empresarial legítima de tales privilegios. Todos los visitantes han de presentar su identificación y deberán firmar e ir acompañados de personal autorizado. Consulte el informe SOC 1 Tipo II para conocer los controles específicos relacionados con el acceso físico, la autorización de acceso a los centros de datos y otros controles relacionados. Consulte la norma ISO 27001; anexo A, dominio 9, para obtener información adicional. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.
	s. Contratación de software y hardware. ¿Qué proceso de contratación se utiliza para asegurar que una fuente legítima ha suministrado el software y el hardware de la infraestructura en la cloud y no se los ha modificado malintencionadamente en tránsito?	De conformidad con el estándar ISO 27001, a los recursos de hardware de AWS se les asigna un propietario, de cuyo seguimiento y monitoreo se encarga el personal de AWS con herramientas de administración del inventario propietarias de AWS. El equipo de la cadena de suministro y contratación de AWS mantiene relaciones con todos los proveedores de AWS. Consulte la norma ISO 27001, anexo A, dominio 7, para obtener información adicional. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.

Área clave	¿Tiene preguntas?	RESPUESTA DE AWS
Protección de los datos frente al acceso no autorizado por parte de clientes del proveedor	a. Segregación de los clientes. ¿Qué garantía tengo de que los mecanismos de virtualización y "varios inquilinos" garantizan una segregación lógica y de red suficiente entre varios inquilinos, de forma que un cliente malintencionado que utilice el mismo equipo físico que yo no pueda acceder a mis datos?	Amazon EC2 actualmente utiliza una versión bastante personalizada del hipervisor Xen. Los equipos de intrusión internos y externos evalúan regularmente el hipervisor para detectar las vulnerabilidades nuevas y existentes y los vectores de ataque. Este hipervisor está perfectamente adaptado para mantener un fuerte aislamiento entre las máquinas virtuales invitadas. Durante las evaluaciones y auditorías, los auditores independientes evalúan con regularidad la seguridad del hipervisor Xen de AWS. Todos los datos almacenados por AWS en nombre de los clientes tienen capacidades sólidas de control y seguridad de aislamiento de organizaciones. Los clientes mantienen el control y la titularidad de sus datos, por lo que son responsables de cifrarlos. AWS permite a los clientes utilizar sus propios mecanismos de cifrado prácticamente para todos los servicios, entre otros, S3, EBS y EC2. También se cifran las sesiones de VPC. Amazon S3 también ofrece a los clientes la opción de utilizar el cifrado del servidor. Consulte el documento técnico Riesgos y conformidad de AWS para obtener más detalles. Este está disponible en http://aws.amazon.com/security.
	b. Debilitamiento de mi nivel de seguridad. ¿En qué medida el uso de la infraestructura en la cloud del proveedor debilitaría el nivel de seguridad de la red actual de mi agencia? ¿El proveedor me anunciaría como uno de sus clientes sin mi consentimiento expreso, ayudando así a un adversario que me tiene como objetivo?	Los clientes de AWS se consideran confidenciales y no se harían públicos detalles de los clientes sin su consentimiento expreso. Amazon Virtual Private Cloud (Amazon VPC) le permite aprovisionar una sección aislada de forma lógica de la cloud de Amazon Web Services (AWS), donde puede lanzar recursos de AWS en una red virtual que usted defina. Puede controlar todos los aspectos del entorno de red virtual, incluida la selección de su propio rango de direcciones IP, la creación de subredes y la configuración de tablas de enrutamiento y puertas de enlace de red.
	c. Servidores dedicados. ¿Tengo algún control sobre en qué equipo físico se ejecutan mis máquinas virtuales? ¿Puedo pagar más dinero para asegurarme de que ningún otro cliente pueda utilizar el mismo equipo físico que yo, por ejemplo servidores dedicados o cloud virtual privada?	VPC permite a los clientes lanzar instancias de Amazon EC2 que estén físicamente aisladas a nivel del hardware host; se ejecutarán en hardware dedicado a un solo inquilino. Una VPC se puede crear con una propiedad "dedicada", en cuyo caso todas las instancias lanzadas en la VPC utilizarán esta función. De forma alternativa, una VPC puede crearse con una propiedad "predeterminada", pero los clientes pueden especificar la propiedad "dedicada" para instancias particulares lanzadas dentro de la VPC.
	d. Saneamiento de soportes. Cuando elimino fragmentos de mis datos, ¿qué procesos se emplean para desinfectar los medios de almacenamiento antes de ponerlos a disposición de otro cliente? ¿El ISM de DSD considera adecuados estos procesos?	Los clientes preservan la titularidad y el control de su contenido, y ofrecen a sus clientes la posibilidad de eliminar sus datos. Cuando un dispositivo de almacenamiento alcanza el final de su vida útil, los procedimientos de AWS incluyen un proceso de retirada diseñado para prevenir que los datos de los clientes queden expuestos al acceso de personas no autorizadas. AWS utiliza las técnicas detalladas en DoD 5220.22-M ("Manual de operaciones del programa de seguridad industrial nacional") o NIST 800-88 ("Directrices para el saneamiento de soportes") para destruir datos como parte del proceso de retirada. En caso de que no se pueda retirar un dispositivo de hardware con estos procedimientos, el dispositivo se desmagnetizará o destruirá físicamente de conformidad con las prácticas estándar del sector. Consulte el documento técnico de información general sobre los procesos de seguridad de AWS para obtener más información, que se encuentra disponible en http://aws.amazon.com/security.

Área clave	¿Tiene preguntas?	RESPUESTA DE AWS
Protección de los datos frente al acceso no autorizado por parte de empleados deshonestos del proveedor	a. Administración de las claves de cifrado de los datos. ¿El proveedor conoce la contraseña o la clave que se utiliza para descifrar mis datos, o soy yo quien cifra y descifra los datos en mi equipo de forma que el proveedor solo tiene acceso a datos cifrados?	Los clientes de AWS administran su propio cifrado a menos que estén utilizando el servicio de cifrado del servidor de AWS. En este caso, AWS crea una clave de cifrado exclusiva para cada inquilino. Consulte el documento técnico de información general sobre los procesos de seguridad de AWS para obtener más información, que se encuentra disponible en http://aws.amazon.com/security.
	b. Selección de los empleados del proveedor. ¿Qué controles y procesos de selección realiza el proveedor para asegurarse de que sus empleados son de confianza?	AWS comprueba los antecedentes penales de conformidad con la legislación aplicable, como parte de las prácticas de preselección de empleados a fin de que estos se adecuen al cargo y al nivel de acceso del empleado a las instalaciones de AWS.
	c. Auditoría de los empleados del proveedor. ¿Qué sistema de administración de acceso e identidades utilizan los empleados del proveedor? ¿Qué proceso de auditoría se utiliza para registrar y revisar las acciones que realizan los empleados del proveedor?	De conformidad con los estándares ISO 27001, AWS ha establecido políticas y procedimientos formales para delinear los estándares mínimos de acceso lógico a los recursos de AWS. En el informe SOC 1, Tipo 2, de AWS, se describen los controles existentes para administrar la provisión de acceso a los recursos de AWS. Consulte el documento técnico de información general sobre los procesos de seguridad de AWS para obtener más información, que se encuentra disponible en http://aws.amazon.com/security.
	d. Visitantes del centro de datos. ¿Los visitantes de los centros de datos van acompañados en todo momento? ¿Se verifican y registran el nombre y otros detalles personales de todos los visitantes?	Todos los visitantes y contratistas han de presentar su identificación y deberán firmar e ir acompañados en todo momento de personal autorizado. AWS solo ofrece acceso al centro de datos y solo facilita información a los empleados y contratistas que tengan necesidad empresarial legítima de tales privilegios. Cuando un empleado deja de tener necesidad empresarial de tales privilegios, su acceso se revoca de inmediato, incluso aunque siga siendo empleado de Amazon o de Amazon Web Services. El acceso físico a los centros de datos de los empleados de AWS está sujeto a logs y auditorías rutinarios.
	e. Manipulación física por parte de los empleados del proveedor. ¿El cableado de red está instalado profesionalmente de acuerdo con los estándares australianos o unos estándares aceptables internacionalmente para ayudar a evitar que los empleados del proveedor conecten accidentalmente cables a los equipos equivocados, y para ayudar a subrayar rápidamente cualquier intento deliberado por parte de los empleados del proveedor de manipulación del cableado?	Los controles de seguridad física incluyen, pero no se limitan a, controles perimetrales como vallas, muros, personal de seguridad, videovigilancia, sistemas de detección de intrusiones y otros medios electrónicos. Esto incluye una protección adecuada de los cables de red. En el informe SOC 1, Tipo 2, de AWS, se ofrecen detalles adicionales acerca de las actividades de control específicas que ejecuta AWS. Consulte la norma ISO 27001; anexo A, dominio 9, para obtener información adicional. Un auditor independiente ha validado y certificado AWS a fin de confirmar que cumple la norma de certificación ISO 27001.

Área clave	¿Tiene preguntas?	RESPUESTA DE AWS
	f. Subcontratistas del proveedor. ¿Las respuestas a estas preguntas son igualmente válidas para todos los subcontratistas del proveedor?	La concesión de acceso a proveedores y contratistas se administra de la misma forma que para los empleados y contratistas, y el departamento de Recursos Humanos (RR. HH.), el de Operaciones Corporativas y los propietarios de servicios comparten esa responsabilidad. Los proveedores están sujetos a los mismos requisitos de acceso que los empleados.
Administración de las incidencias de seguridad	a. Soporte técnico puntual del proveedor. ¿El proveedor está localizable rápidamente y es receptivo a las solicitudes de soporte? ¿El tiempo máximo de respuesta aceptable está reflejado en el SLA o no es más que un reclamo de marketing que dice que el proveedor hará todo lo posible? ¿El soporte técnico se ofrece localmente, desde un país extranjero o desde varios países extranjeros para armonizar los horarios de atención? ¿Qué mecanismos utiliza el proveedor para entender en tiempo real el nivel de seguridad que necesito según mi uso de los servicios del proveedor, de forma que este pueda ofrecer soporte técnico?	AWS Support es un canal de soporte personalizado y de respuesta rápida que presta servicios las 24 horas del día, los 7 días de la semana, durante los 365 días del año; además, cuenta con ingenieros de soporte técnico con experiencia. El servicio ayuda a clientes de todo tamaño y capacidades técnicas para que puedan utilizar de forma satisfactoria los productos y las características de Amazon Web Services. Todas las capas de AWS Support ofrecen a los clientes de AWS Infrastructure Services una cantidad ilimitada de casos de asistencia, con pago mensual y sin acuerdos de larga duración. Los cuatro niveles ofrecen a desarrolladores y negocios la flexibilidad de elegir un nivel de soporte conforme a sus necesidades específicas.
	b. Plan de respuesta ante incidencias del proveedor. ¿El proveedor cuenta con un plan de respuesta ante incidencias de seguridad en el que se especifique cómo detecta y responde ante las incidencias de seguridad, de manera similar a los procedimientos de administración de incidencias detallados en el ISM de DSD? ¿Puedo examinar una copia?	AWS ha implementado un programa y una política formales y documentados de respuesta a incidencias. La política aborda el propósito, el ámbito de aplicación, las funciones, las responsabilidades y el compromiso de la dirección, y se desarrolló de conformidad con los estándares ISO 27001 y NIST 800-53. A continuación se describe el enfoque de tres fases que AWS implementó para administrar las incidencias: 1. Fase de activación y notificación: las incidencias de AWS empiezan con la detección de un evento. Este evento puede proceder de varias fuentes, incluidas: - Métricas y alarmas: AWS es capaz de reconocer las situaciones excepcionales. La mayoría de los problemas se detectan rápidamente con un monitoreo las 24 horas del día, los 7 días de la semana, durante los 365 días del año, y alarmas procedentes de métricas en tiempo real y paneles de servicios. La mayoría de las incidencias se detectan de esta manera. AWS utiliza alarmas con indicadores tempranos para identificar de forma proactiva los problemas que pueden afectar en última instancia a los clientes. - Vale de problema introducido por un empleado de AWS - Llamadas a la línea telefónica de asistencia técnica, que está disponible las 24 horas del día, los 7 días de la semana, durante los 365 días del año. Si el evento cumple los criterios de incidencia, el ingeniero de soporte de guardia correspondiente iniciará una intervención mediante la herramienta de administración de eventos de AWS para localizar a las personas encargadas de la resolución según el programa (por ejemplo, el equipo de seguridad). Estas personas realizarán un análisis de la incidencia a fin de determinar si es necesario involucrar a más personas y averiguar la raíz aproximada del problema. 2. Fase de recuperación: las personas encargadas de la resolución realizarán soporte técnico reactivo para tratar de resolver la incidencia. Una vez que se ha abordado la solución de problemas, el soporte técnico reactivo y los componentes afectados, el coordinador de la llamada asignará los pasos que hay que seguir a continuación en cuanto a documentación y acciones de seguimiento, y dará por terminada la intervención.

		3. Fase de reconstitución: una vez completadas las actividades de corrección pertinentes, el coordinador declarará finalizada la fase de recuperación. Se asignarán al equipo correspondiente el análisis final y un análisis detallado de la causa de la incidencia. La alta dirección examinará los resultados del análisis final y las acciones pertinentes como cambios de diseño, etc. se incluirán en un documento de corrección de errores (COE); también se hará un seguimiento de las mismas hasta su finalización. Además de los mecanismos de comunicación interna explicados anteriormente, AWS también ha implementado varios métodos de comunicación externa para prestar asistencia a su cartera de clientes y a la comunidad. El equipo de atención al cliente dispone de mecanismos para recibir notificaciones sobre problemas operativos que afecten a la experiencia de los clientes. El equipo de atención al cliente realiza el mantenimiento del "Panel de estado del servicio" para que se encuentre disponible a fin de advertir al cliente de cualquier problema que pueda tener un gran impacto. Los auditores independientes externos revisan el programa de administración de incidencias de AWS durante las auditorías de nuestra conformidad con SOC, PCI DSS, ISO 27001 and FedRAMP. **Consulte el documento técnico de seguridad de la cloud de AWS** para obtener información adicional, que se encuentra disponible en http://aws.amazon.com/security.
	c. Formación de los empleados del proveedor. ¿Qué cualificaciones, certificaciones y formación periódica de sensibilización sobre la seguridad de la información han de tener los empleados del proveedor para saber cómo utilizar los sistemas del proveedor de forma segura y para identificar posibles incidencias de seguridad?	De conformidad con el estándar ISO 27001, todos los empleados de AWS realizan una capacitación periódica sobre la seguridad de la información; para completarla es necesario enviar un acuse de recibo. Las auditorías de conformidad se realizan periódicamente a fin de validar que los empleados puedan conocer y seguir las políticas establecidas. Consulte el documento técnico de información general sobre los procesos de seguridad de AWS para obtener más información, que se encuentra disponible en http://aws.amazon.com/security.
	d. Notificación de las incidencias de seguridad. ¿El proveedor me notificará a través de comunicaciones seguras las incidencias de seguridad que sean más graves que un umbral acordado, sobre todo en aquellos casos en los que el proveedor pueda ser responsable? ¿El proveedor notificará automáticamente a las autoridades competentes o a otras autoridades, las cuales pueden confiscar los equipos informáticos utilizados para almacenar o procesar mis datos?	La notificación de las incidencias de seguridad se realiza caso por caso y tal y como lo establece la legislación aplicable. Todas las notificaciones se realizan a través de comunicaciones seguras.

Área clave	¿Tiene preguntas?	RESPUESTA DE AWS
	e. Alcance del apoyo técnico del proveedor. ¿Cuánta ayuda me ofrecerá el proveedor con las investigaciones si se produce una infracción de seguridad como una divulgación no autorizada de mis datos, o si es necesario realizar un descubrimiento de pruebas electrónico legal?	AWS ofrece la infraestructura y los clientes administran todo lo demás, como el sistema operativo, la configuración de red y las aplicaciones instaladas. Los clientes son responsables de responder según corresponda a los procedimientos legales que impliquen la identificación, la recopilación, el procesamiento, el análisis y la elaboración de los documentos electrónicos que almacenan o procesan con AWS. Previa solicitud, AWS puede colaborar con los clientes que requieran la asistencia de AWS en procedimientos legales.
	f. Mi acceso a los registros. ¿Cómo obtengo acceso a los registros de auditoría con sincronización de tiempo y a otros registros para realizar una investigación forense, y cómo se crean y almacenan los registros que serán pruebas válidas en un tribunal de justicia?	Los clientes mantienen el control de los sistemas operativos invitados, el software y las aplicaciones con los que cuentan, por lo que además son responsables de realizar un monitoreo lógico de las condiciones de estos sistemas. De conformidad con los estándares ISO 27001, los sistemas de información de AWS utilizan relojes internos del sistema sincronizados a través del Network Time Protocol (NTP, protocolo de tiempo de redes). AWS CloudTrail ofrece una solución simple para registrar la actividad de los usuarios, lo que ayuda a reducir la carga que supone ejecutar un sistema de registro complejo. Consulte aws.amazon.com/cloudtrail para obtener información adicional. AWS CloudWatch proporciona el monitoreo de los recursos de la cloud de AWS y de las aplicaciones que los clientes ejecutan en AWS. Consulte aws.amazon.com/cloudwatch para obtener información adicional. AWS también publica la información más actualizada sobre la disponibilidad del servicio en el Panel de estado del servicio. Visite status.aws.amazon.com.
	g. Compensación por las incidencias de seguridad. ¿Cómo me compensará adecuadamente el proveedor si las acciones del proveedor o el uso de software o hardware defectuoso contribuyen a una infracción de seguridad?	El programa, los planes y los procedimientos para responder a las incidencias de AWS se han desarrollado en consonancia con el estándar ISO 27001. En el informe SOC 1, Tipo 2, de AWS, se ofrecen detalles adicionales acerca de las actividades de control específicas que ejecuta AWS. En el documento técnico de información general sobre los procesos de seguridad de AWS (disponible en http://aws.amazon.com/security) se facilita información adicional.

Área clave	¿Tiene preguntas?	RESPUESTA DE AWS
	h. Vertido de datos. Si los datos que considero demasiado confidenciales como para almacenarlos en la cloud se ubican accidentalmente en la cloud, lo que se conoce como vertido de datos, ¿cómo se eliminarán los datos vertidos mediante técnicas forenses de saneamiento? ¿La parte correspondiente de los medios de almacenamiento físico se pone a cero siempre que se eliminan datos? En caso negativo, ¿cuánto tiempo tardan los clientes en sobrescribir los datos eliminados como parte de una operación normal, teniendo en cuenta que las clouds suelen tener gran cantidad de capacidad de almacenamiento sin utilizar? ¿Los datos vertidos se pueden eliminar pericialmente de los medios de backup? ¿En qué otros sitios se almacenan los datos vertidos? ¿Se pueden eliminar pericialmente?	Los clientes preservan la titularidad y el control de su contenido. Todos los datos almacenados por AWS en nombre de los clientes tienen capacidades sólidas de control y seguridad de aislamiento de organizaciones. AWS permite a los clientes utilizar sus propios mecanismos de cifrado prácticamente para todos los servicios, entre otros, S3, EBS y EC2. Los túneles IPSec con VPC también están cifrados. Amazon S3 también ofrece a los clientes la opción de utilizar el cifrado del servidor. Consulte el documento técnico Riesgos y conformidad de AWS para obtener más detalles. Este está disponible en http://aws.amazon.com/security. Consulte el documento técnico Riesgos y conformidad de AWS para obtener más detalles. Este está disponible en http://aws.amazon.com/security.

Apéndice C: Glosario de términos

Autenticación: la autenticación es el proceso por el que se determina si alguien o algo es realmente quien o lo que se supone que es.

Zona de disponibilidad: las ubicaciones de Amazon EC2 se componen de regiones y zonas de disponibilidad. Las zonas de disponibilidad son regiones diferentes que están diseñadas para estar aisladas de errores que se produzcan en otras zonas de disponibilidad, y que proporcionan conectividad de red de baja latencia a otras Zonas de disponibilidad de la misma región.

DSS: el estándar de seguridad de datos (Data Security Standard, DSS) del sector de las tarjetas de pago (Payment Card Industry, PCI) es un estándar internacional de seguridad de la información que el Payment Card Industry Security Standards Council creó y administra.

EBS: Amazon Elastic Block Store (EBS) proporciona volúmenes de almacenamiento de nivel de bloque diseñados para su uso con instancias de Amazon EC2. Los volúmenes de Amazon EBS son de almacenamiento fuera de la instancia que persiste con independencia de la duración de una instancia.

FedRAMP[sm]: el Federal Risk and Authorization Management Program (FedRAMP[sm]) es un programa gubernamental que proporciona un enfoque estandarizado para la evaluación, la autorización y el monitoreo continuo de la seguridad de los productos y servicios en la cloud. FedRAMP[sm] es de uso obligatorio para las implementaciones y los modelos de servicios en la cloud de las agencias federales en los niveles de impacto de riesgos bajo y moderado.

FISMA: la Ley sobre la Administración de la Seguridad de la Información (Federal Information Security Management Act) de 2002. La ley prevé que cada organismo federal desarrolle, documente y aplique un programa de ámbito institucional para ofrecer la seguridad de la información y de todos los sistemas de información que respaldan las operaciones y los recursos de la institución, incluidos los que facilitan o administran otras instituciones, otros contratistas u otras fuentes.

FIPS 140-2: la Publicación 140-2 del Federal Information Processing Standard (FIPS) es un estándar de seguridad del gobierno de EE. UU. que especifica los requisitos de seguridad para los módulos criptográficos que protegen información confidencial.

GLBA: la Ley de Gramm–Leach–Bliley (GLB o GLBA), también conocida como la Ley de Modernización de los Servicios Financieros de 1999, establece los requisitos que deben cumplir las instituciones financieras con respecto a, entre otras cosas, la divulgación de información privada de los clientes y la protección frente a amenazas de seguridad e integridad de los datos.

HIPAA: la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA) de 1996 requiere el establecimiento de estándares nacionales para las transacciones sanitarias electrónicas e identificadores nacionales para los proveedores, planes de seguros médicos y empresarios. Las disposiciones sobre la simplificación de la administración también tratan la seguridad y la privacidad de los datos relativos a la salud. Los estándares pretenden mejorar la eficiencia y eficacia del sistema de atención sanitaria nacional al fomentar el uso generalizado del intercambio electrónico de datos en el sistema estadounidense de atención sanitaria.

Hipervisor: un hipervisor, también denominado monitor de máquina virtual (VMM), es un software de virtualización de plataformas de software o hardware que permite que varios sistemas operativos se ejecuten en un equipo host de forma simultánea.

IAM: AWS Identity and Access Management (IAM) permite que un cliente cree múltiples usuarios y administre los permisos para cada uno de estos usuarios dentro de su cuenta de AWS.

ITAR: el Reglamento sobre Tráfico Internacional de Armas (ITAR) es un conjunto de reglamentos del gobierno de los Estados Unidos que controlan la exportación e importación de artículos y servicios relacionados con la defensa incluidos en la Lista de Municiones de Estados Unidos (USML, United States Munitions List). Los contratistas y las instituciones gubernamentales deben cumplir el ITAR y restringir el acceso a los datos protegidos.

ISAE 3402: el International Standards for Assurance Engagements No. 3402 (ISAE 3402) es el estándar internacional de auditorías. Lo presentó el consejo International Auditing and Assurance Standards Board (IAASB), un organismo responsable de establecer estándares dentro de la federación internacional de contables International Federation of Accountants (IFAC). ISAE 3402 actualmente constituye el nuevo estándar reconocido a nivel mundial para informar de las garantías en las organizaciones de servicios.

ISO 9001: la certificación AWS 9001 de ISO ayuda directamente a los clientes que desarrollan, migran y operan en la cloud de AWS sus sistemas de TI con control de calidad. Los clientes pueden utilizar los informes de conformidad de AWS para demostrar que disponen de sus propios programas ISO 9001 y programas de calidad específicos del sector, como GxP para las ciencias de la salud, ISO 13485 para dispositivos médicos, AS9100 para el sector aeroespacial e ISO/TS 16949 para el sector del automóvil. Los clientes de AWS que no poseen requisitos de sistema de calidad pueden beneficiarse de la seguridad y transparencia adicionales que proporciona la certificación ISO 9001.

ISO 27001: ISO/IEC 27001 es un estándar del Sistema de Administración de la Seguridad de la Información (ISMS) publicado por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (CEI). La ISO 27001 oficialmente especifica un sistema de administración que pretende ejercer un control de administración explícito de la seguridad de la información. Al tratarse de una especificación oficial, significa que exige requisitos específicos. Las organizaciones que proclamen haber adoptado la ISO/IEC 27001 pueden ser auditadas y certificadas de conformidad con el estándar.

NIST: Instituto Nacional de Normalización y Tecnología. Este organismo establece estándares de seguridad detallados según las necesidades del sector o de los programas gubernamentales. A efectos de conformidad con la FISMA, las instituciones han de atenerse a los estándares del NIST.

Objeto: las entidades fundamentales almacenadas en Amazon S3. Los objetos se componen de datos de objetos y metadatos. La parte de datos es opaca para Amazon S3. Los metadatos son conjuntos de pares de valores de nombres que describen el objeto. Estos incluyen algunos metadatos predeterminados como la fecha de la última modificación y los metadatos HTTP estándar como el tipo de contenido. El desarrollador también puede especificar metadatos personalizados en el momento en que se almacena el objeto.

PCI: se refiere al Payment Card Industry Security Standards Council, un consejo independiente constituido originalmente por American Express, Discover Financial Services, JCB, MasterCard Worldwide y Visa International, para administrar la continua evolución del estándar de seguridad de los datos del sector de las tarjetas de pago (DSS del PCI).

QSA: el Consejo de Estándares de Seguridad del PCI concede la designación Asesor de seguridad cualificado (QSA) del sector de las tarjetas de pago (PCI) a aquellas personas que cumplen determinados requisitos de cualificación y están autorizadas a realizar evaluaciones de conformidad de PCI.

SAS 70: la Declaración de Estándares de Auditoría (SAS) N.º 70, Organizaciones de Servicios, es una declaración de auditoría publicada por la Comisión Internacional de Estándares de Auditoría y Seguros del American Institute of Certified Public Accountants (AICPA). En la SAS 70 se ofrece orientación a los auditores de servicios para evaluar los controles internos de una organización de servicios (como AWS) y para presentar un informe del auditor del servicio. En la SAS 70 también se ofrece orientación a los auditores de declaraciones financieras de una entidad que utiliza una o varias organizaciones de servicios. El informe SAS 70 se ha reemplazado por el informe Service Organization Controls 1.

Service: software o capacidad informática que se presta a través de una red (por ejemplo, EC2, S3, VPC, etc.).

Acuerdo de nivel de servicios (SLA): un acuerdo de nivel de servicios forma parte de un acuerdo de servicios en el que se define formalmente el nivel de servicio. El SLA se utiliza para referirse al tiempo o al rendimiento contratado de prestación del servicio.

SOC 1: el informe Controles de las Organizaciones de Servicios 1 (SOC 1) Tipo II, denominado anteriormente Declaración de Estándares de Auditoría (SAS) Nº 70, Organizaciones de Servicios (conocido anteriormente como el informe SSAE 16), es un estándar de auditoría reconocido ampliamente desarrollado por el American Institute of Certified Public Accountants (AICPA). Al estándar internacional se hace referencia como International Standards for Assurance Engagements N.º 3402 (ISAE 3402).

SSAE 16 [fuera de uso]: Statement on Standards for Attestation Engagements No. 16 (SSAE 16) es un estándar de certificación publicado por la Comisión Internacional de Estándares de Auditoría y Seguros del American Institute of Certified Public Accountants (AICPA). Este estándar aborda las actividades que lleva a cabo un auditor de servicios para informar sobre los controles de las organizaciones que prestan servicios a entidades de usuarios, en las que los controles de una organización de servicios son probablemente importantes para el control interno sobre información financiera (ICFR) de las entidades de usuarios. SSAE 16 reemplaza perfectamente al estándar Statement on Auditing Standards N.º 70 (SAS 70) durante los períodos de información del auditor del servicio que terminan el 15 de junio de 2011 o después.

SOC 2: los informes Controles de las organizaciones de servicios 2 (SOC 2) intentan resolver las necesidades de una amplia gama de usuarios que necesitan comprender los controles internos de una organización de servicios en lo referente a la seguridad, disponibilidad, integridad durante el procesamiento, confidencialidad y privacidad. Estos informes se realizan con la Guía de AICPA: Reporting on Controls at a Service Organizations Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy y están diseñados para que los usen las partes interesadas (por ejemplo, clientes, reguladores, socios empresariales, proveedores, directores) de la organización de servicios que entienden perfectamente dicha organización y sus controles internos.

SOC 3: los informes Controles de las organizaciones de servicios 3 (SOC 3) están diseñados para resolver las necesidades de los usuarios que desean tener una garantía de los controles de una organización de servicios relativos a la seguridad, disponibilidad, integridad durante el procesamiento, confidencialidad o privacidad, pero no tienen la necesidad o el conocimiento necesario para hacer un uso eficaz de un informe SOC 2. Estos informes se elaboran usando los principios, los criterios y las ilustraciones de los servicios de confianza de AICPA/Canadian Institute of Chartered Accountants (CICA) en relación con la seguridad, la disponibilidad, la integridad del procesamiento, la confidencialidad y la privacidad. Habida cuenta de que se trata de informes de uso general, los informes SOC 3 pueden distribuirse de manera gratuita o publicarse en un sitio web como sello.

Instancia virtual: después de haber lanzado una AMI, se hace referencia al sistema de ejecución resultante como una instancia. Todas las instancias basadas en la misma AMI se inician de forma idéntica y la información que contienen se pierde cuando se terminan las instancias o cuando estas fallan.

Historial de versiones

Enero de 2016

- Se agregó el Programa de Cumplimiento de GxP.
- Se agregó la región número doce (Asia Pacífico-Seúl)

Diciembre de 2015

- Resúmenes de actualizaciones de certificaciones y acreditaciones independientes
- Se agregó la certificación del estándar ISO 27017.
- Se agregó la certificación del estándar ISO 27018.
- Se agregó la región número once (China- Pekín)

Noviembre de 2015

- Se actualizó a la versión CSA v3.0.1.

Agosto de 2015

- Actualizaciones a los servicios que recaen dentro del ámbito de aplicación para PCI 3.1
- Actualizaciones a las regiones que recaen dentro del ámbito de aplicación para PCI 3.1

Mayo de 2015

- Se agregó la región número diez (UE-Fráncfort)
- Actualizaciones a los servicios que recaen dentro del ámbito de aplicación para SOC 3
- Se sacó de uso la SSAE 16 en este idioma.

Abril de 2015

- Actualizaciones a los servicios que recaen dentro del ámbito de aplicación para FedRAMP^{sm}, HIPAA, SOC 1, ISO 27001, ISO 9001

Febrero de 2015

- Actualizaciones a los puntos de enlace de VPN de FIPS 140-2 y equilibradores de carga con terminación SSL
- Actualizaciones al texto sobre PCI DSS

Diciembre de 2014

- Resúmenes de actualizaciones de certificaciones y acreditaciones independientes

Versión de noviembre de 2013

- Cambios en el texto sobre el cifrado del túnel IPsec

Versión de junio de 2013

- Resúmenes de actualizaciones de certificaciones y acreditaciones independientes
- Actualizaciones el Apéndice C: glosario de términos
- Modificaciones menores de formato

Versión de enero de 2013

- Resúmenes de modificaciones de certificaciones y acreditaciones independientes

Versión de noviembre de 2012

- Modificaciones de contenido y ámbito de aplicación de la certificación actualizado
- Referencia incorporada a SOC 2 y MPAA

Versión de julio de 2012

- Modificaciones de contenido y ámbito de aplicación de la certificación actualizado
- Incorporación del cuestionario Consensus Assessments Initiative Questionnaire de CSA (apéndice A)

Versión de enero de 2012

- Modificaciones de menor importancia del contenido basadas en el ámbito de aplicación de la certificación actualizado
- Cambios gramaticales de menor importancia

Versión de diciembre de 2011

- Cambio en la sección Certificaciones y acreditación de terceros para reflejar el estándar SOC 1/SSAE 16, el nivel FISMA Moderate, el Reglamento Internacional de Tráfico de Armas y FIPS 140-2
- Incorporación del cifrado del servidor de S3
- Temas adicionales añadidos acerca de cloud computing

Versión de mayo de 2011

- Versión inicial

Avisos