Certificações, programas, relatórios e atestados de terceiros da AWS

Janeiro de 2017

Avisos

Este documento é fornecido apenas para fins informativos. Ele relaciona as atuais ofertas de produtos e práticas da AWS a contar da data de emissão deste documento, que estão sujeitas a alterações sem aviso prévio. Os clientes são responsáveis por fazer sua própria avaliação independente das informações deste documento e de qualquer uso dos produtos ou serviços da AWS, cada um dos quais é fornecido “no estado em que se encontra”, sem garantia de qualquer tipo, expressa ou implícita. Este documento não cria quaisquer garantias, representações, compromissos contratuais ou condições da AWS, suas afiliadas, seus fornecedores ou licenciadores. As responsabilidades da AWS com seus clientes são controladas pelos contratos da AWS, e este documento não modifica nem faz parte de qualquer contrato entre a AWS e seus clientes.

Índice

Resumo

A AWS contrata órgãos externos de certificação e auditores independentes para fornecer aos clientes um grande volume de informações sobre as políticas, os processos e os controles estabelecidos e operados pela AWS.

CJIS

AWS está em conformidade com o padrão CJIS (Serviços de Informações da Justiça Criminal) do FBI. Assinamos contratos de segurança de CJIS com nossos clientes, incluindo a permissão ou execução de quaisquer verificações de antecedentes de funcionários necessárias, de acordo com a Política de segurança do CJIS.

Os clientes da área de execução da lei (e parceiros que administram o CJI) estão aproveitando os serviços da AWS para melhorar a segurança e a proteção dos dados CJI, usando os serviços de segurança e os recursos avançados da AWS, tais como registro de atividades (AWS CloudTrail), criptografia de dados em movimento e em repouso (Server-Side Encryption do S3 com a opção de trazer a sua própria chave), gerenciamento de chaves e proteção abrangentes (AWS Key Management Service e CloudHSM) e gerenciamento integrado de permissões (gerenciamento de identidades federado IAM, autenticação multifator).

A AWS criou um manual do CJIS em um formato de modelo de plano de segurança alinhado às áreas de políticas do CJIS. Além disso, foi desenvolvido um whitepaper sobre o CJIS para ajudar a guiar clientes em sua jornada de adoção da nuvem.

Visite a página principal do CJIS em https://aws.amazon.com/compliance/cjis/.

CSA

Em 2011, o Cloud Security Alliance (CSA – Aliança de segurança da nuvem) lançou o STAR, uma iniciativa que incentiva a transparência nas práticas de segurança dentro dos provedores de nuvem. O CSA Security, Trust & Assurance Registry (STAR – Segurança, confiança e registro de seguro) é um registro gratuito, acessível ao público, que documenta os controles de segurança fornecidos por várias ofertas de computação em nuvem, ajudando os usuários a avaliarem a segurança dos provedores de nuvem que utilizam atualmente ou que estão considerando contratar. A AWS é registrada pelo CSA STAR e concluiu o CAIQ (Questionário da iniciativa de avaliação de consenso) da CSA (Cloud Security Alliance). Esse CAIQ publicado pela CSA fornece uma forma de referenciar e documentar quais controles de segurança existem nas ofertas de infraestrutura como serviço da AWS. O CAIQ fornece 298 perguntas que um auditor de nuvem e um cliente de nuvem podem querer fazer a um provedor de nuvem.

Consulte o Questionário da iniciativa de avaliação de consenso da CSA.

Cyber Essentials Plus

Cyber Essentials Plus é um sistema de certificação reconhecido pela indústria e apoiado pelo governo do Reino Unido que foi introduzido no país para ajudar as organizações a demonstrar segurança operacional contra ataques cibernéticos comuns.

Ele demonstra a linha de base de controle que a AWS implementa para reduzir o risco de ameaças comuns baseadas na Internet, dentro do contexto do governo do Reino Unido de "10 passos para a segurança cibernética". É apoiado pela indústria, incluindo a Federação das Pequenas Empresas, a Confederação da Indústria Britânica e diversas organizações de seguros que oferecem incentivos para as empresas que contam com esta certificação.

Cyber Essentials estabelece os controles técnicos necessários; o quadro de garantia relacionado mostra como o processo de verificação independente trabalha pela certificação do Cyber Essentials Plus através de uma avaliação externa anual realizada por um avaliador credenciado. Devido à natureza regional da certificação, o seu escopo é limitado à região da UE (Irlanda).

DoD SRG níveis 2 e 4

O Modelo de Segurança de Nuvem (SRG) do Departamento de Defesa (DoD) oferece uma avaliação formalizada e um processo de autorização para os provedores de serviço na nuvem (CSPs) obterem uma autorização provisória do DoD, que posteriormente pode ser aproveitada pelos clientes do DoD. Uma autorização provisória sob o SRG oferece uma certificação reutilizável que atesta nossa conformidade com as normas do DoD, reduzindo o tempo necessário para que um proprietário de missão do DoD avalie e autorize um dos seus sistemas para operação na AWS. A AWS atualmente detém as autorizações provisórias nos níveis 2 e 4 da SRG.

Informações adicionais das linhas de base de controle de segurança definidas para os níveis 2, 4, 5, e 6 podem ser encontradas em: http://iase.disa.mil/cloud_security/Pages/index.aspx.

Visite a página principal do DoD em https://aws.amazon.com/compliance/dod/.

FedRAMPSM

A AWS é um provedor de serviço na nuvem em conformidade com o FedRAMPsm (Federal Risk and Authorization Management Program). A AWS concluiu os testes realizados por uma 3PAO (Third Party Assessment Organization) acreditada pelo FedRAMPsm e recebeu duas ATOs (Authority to Operate) pelo Departamento de Saúde e Serviços Humanos dos EUA (HHS) depois de demonstrar conformidade com os requisitos do FedRAMPsm em nível de impacto moderado. Todas as agências do governo americano podem aproveitar os pacotes de ATO para agências da AWS armazenados no repositório do FedRAMPsm para avaliar a AWS em relação às suas aplicações e cargas de trabalho, fornecer autorizações para usar a AWS e fazer a transição de cargas de trabalho dentro do ambiente da AWS. As duas ATOs de agência do FedRAMPsm englobam todas as regiões dos EUA [a região AWS GovCloud (EUA) e as regiões AWS Leste e Oeste dos EUA].

Os seguintes serviços fazem parte do conjunto de acreditação nas regiões citadas acima:

- **Amazon Redshift** – o Amazon Redshift é um serviço de armazenamento de dados rápido, totalmente gerenciado e em escala de petabytes, que torna mais simples e acessível a análise eficiente de todos os seus dados usando as ferramentas de inteligência de negócios de que você dispõe. Para obter mais informações, clique aqui.
- **Amazon Elastic Compute Cloud (Amazon EC2)** – o Amazon EC2 disponibiliza uma capacidade computacional redimensionável na nuvem. Ele foi projetado para facilitar a computação na escala da web para os desenvolvedores. Para obter mais informações, clique aqui.
- **Amazon Simple Storage Service (S3)** – o Amazon S3 fornece uma interface simples de serviço web que pode ser usada para armazenar e recuperar qualquer quantidade de dados, a qualquer momento, de qualquer lugar na web. Para obter mais informações, clique aqui.
- **Amazon Virtual Private Cloud (VPC)** – o Amazon VPC possibilita a você provisionar uma seção da nuvem da AWS isolada logicamente onde você pode executar recursos da AWS em uma rede virtual que você mesmo define. Para obter mais informações, clique aqui.

- **Amazon Elastic Block Store (EBS)** – o Amazon EBS fornece volumes de armazenamento altamente disponíveis, confiáveis e previsíveis que podem ser conectados a uma instância do Amazon EC2 em execução e expostos como um dispositivo dentro da instância. Para obter mais informações, clique aqui.
- **AWS Identity and Access Management (IAM)** – o IAM permite que você controle com segurança o acesso aos serviços e recursos da AWS para os seus usuários. Usando o IAM, você pode criar e gerenciar usuários e grupos da AWS e usar permissões para permitir e negar o acesso deles aos recursos da AWS. Para obter mais informações, clique aqui.

Para obter mais informações sobre a conformidade com o FedRAMP^{sm} na AWS, acesse as Perguntas Frequentes sobre o FedRAMP^{sm} em: https://aws.amazon.com/compliance/fedramp/.

FERPA

A Lei da Privacidade e dos Direitos Educacionais da Família (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) é uma lei federal que protege a privacidade dos registros educacionais do estudante. A lei se aplica a todas as escolas que recebem fundos do programa aplicado do Departamento de Educação dos Estados Unidos. FERPA dá aos pais certos direitos com relação aos registros educacionais de seus filhos. Estes direitos são transferidos para o aluno quando ele completa 18 anos ou frequenta uma escola após o ensino médio. Os estudantes a quem os diretos foram transferidos são "estudantes elegíveis".

A AWS habilita entidades abrangidas e os seus associados de trabalho sujeitos ao FERPA a alavancarem o ambiente seguro da AWS para processar, manter e armazenar informações protegidas da educação.

A AWS também oferece um whitepaper sobre a FERPA para os clientes interessados em saber mais sobre como podem aproveitar a AWS para o processamento e armazenamento de dados educacionais.

O whitepaper FERPA Compliance on AWS descreve como as empresas podem usar a AWS para processar sistemas que facilitam a conformidade com a FERPA:

FIPS 140-2

A publicação 140-2 do Federal Information Processing Standard (FIPS) é um padrão de segurança do governo dos EUA que especifica os requisitos de segurança para módulos de criptografia que protegem informações confidenciais. Para oferecer suporte a clientes com requisitos FIPS 140-2, as terminações SSL no AWS GovCloud (EUA) operam usando o hardware validado pela FIPS 140-2. A AWS trabalha com clientes do AWS GovCloud (EUA) para fornecer as informações necessárias para ajudar a gerenciar a conformidade ao usar o ambiente AWS GovCloud (EUA).

FISMA e DIACAP

A AWS permite que os órgãos governamentais dos EUA alcancem e mantenham a conformidade com a [FISMA (Federal Information Security Management Act)]. A infraestrutura da AWS foi avaliada por assessores independentes para diversos sistemas governamentais, como parte do processo de aprovação dos proprietários desses sistemas. Várias organizações civis e do Departamento de defesa (DoD) conseguiram autorizações de segurança para sistemas hospedados na AWS, de acordo com o processo de Estrutura de gerenciamento de riscos (RMF) definido na NIST 800-37 e no Processo de certificação e credenciamento de garantia da informação do DoD (DIACAP).

GxP

GxP é um acrônimo que se refere às regulamentações e orientações aplicáveis às organizações de ciências biológicas que fabricam produtos alimentícios e médicos, como remédios, dispositivos médicos e aplicações de software médicos. A intenção geral dos requisitos de GxP é garantir que os produtos médicos e alimentícios sejam seguros para o consumo e garantir a integridade dos dados usados na tomada de decisão sobre a segurança relacionada aos produtos.

A AWS oferece um whitepaper de GxP que detalha a abordagem abrangente do uso da AWS para sistemas GxP. Este whitepaper oferece orientação quanto ao uso de produtos da AWS no contexto de GxP e o conteúdo foi desenvolvido em conjunto com clientes de dispositivos farmacêuticos e médicos da AWS, bem como parceiros de software, que atualmente usam produtos da AWS nos sistemas GxP validados.

Para obter mais informações sobre o GxP na AWS, entre em contato com o Desenvolvimento de vendas e negócios da AWS.

Para obter informações adicionais, acesse as Perguntas Frequentes sobre a conformidade com o GxP em: https://aws.amazon.com/compliance/gxp-part-11-annex-11/.

HIPAA

A AWS permite que entidades cobertas e seus associados de negócios sujeitos ao U.S. Health Insurance Portability and Accountability Act (HIPAA, Lei de responsabilidade e portabilidade de seguro-saúde dos Estados Unidos) aproveitem o ambiente seguro da AWS para processar, manter e armazenar informações de saúde protegidas. A AWS assinará acordos de associados de negócios com tais clientes. A AWS também oferece um whitepaper sobre a HIPAA para os clientes interessados em saber mais sobre como podem aproveitar a AWS para o processamento e armazenamento de informações de saúde. O whitepaper Architecting for HIPAA Security and Compliance on Amazon Web Services descreve como as empresas podem usar a AWS para processar sistemas que facilitam a conformidade com a HIPAA e a Health Information Technology for Economic and Clinical Health (HITECH, Tecnologia da informação da saúde para a saúde econômica e clínica).

Os clientes podem usar qualquer serviço da AWS em uma conta designada como conta da HIPAA, mas devem somente processar, armazenar e transmitir PHI nos serviços qualificados para a HIPAA definidos no BAA. Há nove serviços elegíveis para HIPAA hoje, incluindo:

- 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) usando apenas mecanismos MySQL e Oracle
- Amazon Simple Storage Service (S3)

A AWS segue um programa de gerenciamento de riscos baseado em padrões para garantir que os serviços qualificados ofereçam suporte específico a processos de segurança, controle e administração exigidos pela HIPAA. Usar esses serviços para armazenar e processar PHI permite que os nossos clientes e a AWS atendam aos requisitos da HIPAA aplicáveis ao nosso modelo de operação com base em utilitários. A AWS prioriza e acrescenta novos serviços qualificados com base na demanda do cliente.

Para obter informações adicionais, consulte nossas Perguntas Frequentes sobre HIPAA Compliance e o whitepaper Architecting for HIPAA Security and Compliance on Amazon Web Services.

IRAP

O Programa de Assessores Registrados de Segurança da Informação (IRAP) permite que os clientes do governo australiano validem os controles apropriados que estão em vigor e determinem o modelo de responsabilidade adequado para responder às necessidades do Manual de Segurança da Informação (ISM) da Australian Signals Directorate (ASD).

O Amazon Web Services concluiu uma avaliação independente que determinou que todos os controles ISM aplicáveis estão em vigor relativamente ao processamento, armazenamento e transmissão de Unclassified (DLM) para o AWS Sydney Region.

Para obter mais informações, consulte as Perguntas Frequentes sobre Conformidade com a IRAP em https://aws.amazon.com/compliance/irap/ e Alinhamento da AWS com as Considerações de Segurança de Computação em Nuvem do ASD (Australian Signals Directorate).

ISO 9001

A AWS obteve a certificação ISO 9001, que oferece suporte direto aos clientes que desenvolvem, migram e operam seus sistemas de TI com controle de qualidade na nuvem da AWS. Os clientes podem usar os relatórios de conformidade da AWS como evidência para seus próprios programas ISO 9001 e para programas de qualidade específicos por setor, como GxP em ciências biológicas, ISO 13485 em dispositivos médicos, AS9100 no setor aeroespacial e ISO/TS 16949 no setor automotivo. Os clientes da AWS que não têm requisitos de sistema da qualidade também se beneficiarão da garantia e transparência adicionais proporcionadas por uma certificação pela ISO 9001.

A ISO 9001 abrange o sistema de gerenciamento de qualidade em um escopo específico de serviços e regiões de operação da AWS (abaixo), que inclui:

- 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 - Web Application Firewall
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- A infraestrutura física subjacente e o ambiente de gerenciamento da AWS

O credenciamento ISO 9001 da AWS cobre as regiões da AWS, incluindo Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon), Oeste dos EUA (Norte da Califórnia), AWS GovCloud (EUA), América do Sul (São Paulo), UE (Irlanda), UE (Frankfurt) e Ásia-Pacífico (Cingapura), Ásia-Pacífico (Sydney) e Ásia-Pacífico (Tóquio).

A ISO 9001:2008 é uma norma global para o gerenciamento da qualidade de produtos e serviços. O padrão 9001 descreve um sistema de gerenciamento da qualidade com base em oito princípios definidos pelo Technical Committee for Quality Management and Quality Assurance da International Organization for Standardization (ISO). Os princípios incluem:

- Foco no cliente
- Liderança
- Envolvimento das pessoas
- Abordagem de processo
- Abordagem sistêmica da gestão
- Melhoria contínua
- Abordagem factual da tomada de decisão
- Relacionamento mutuamente benéfico com fornecedores

É possível baixar a certificação ISO 9001 da AWS de https://d0.awsstatic.com/certifications/iso_9001_certification.pdf.

A AWS fornece informações adicionais e perguntas frequentes sobre sua conformidade com o ISO 9001 em: https://aws.amazon.com/compliance/iso-9001-faqs/.

ISO 27001

A AWS obteve a certificação ISO 27001 do nosso Information Security Management System (ISMS - Sistema de gestão de segurança da informação) que abrange a infraestrutura, datacenters e serviços da AWS como:

- 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 - Web Application Firewall
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- A infraestrutura física subjacente (incluindo a GovCloud) e o Ambiente de Gerenciamento da AWS

A ISO 27001/27002 é um padrão de segurança global amplamente adotado que estabelece os requisitos e as práticas recomendadas para uma abordagem sistemática de gerenciamento de informações da empresa e do cliente, com base em avaliações periódicas de riscos apropriadas e cenários de ameaça em constante mudança. Para obter a certificação, uma empresa deve demonstrar que tem uma abordagem constante e sistemática para gerenciar os riscos de segurança da informação que afetam a confidencialidade, a integridade e a disponibilidade da empresa e das informações do cliente. Essa certificação reforça o compromisso da Amazon de fornecer informações importantes sobre nossas práticas e controles de segurança.

O credenciamento ISO 27001 da AWS cobre as regiões da AWS, incluindo Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon), Oeste dos EUA (Norte da Califórnia), AWS GovCloud (EUA), América do Sul (São Paulo), UE (Irlanda), UE (Frankfurt), Ásia-Pacífico (Cingapura), Ásia-Pacífico (Sydney) e Ásia-Pacífico (Tóquio).

É possível baixar a certificação ISO 27001 da AWS de https://d0.awsstatic.com/certifications/iso_27001_global_certification.pdf.

A AWS fornece informações adicionais e perguntas frequentes sobre sua conformidade com o ISO 27001 em: https://aws.amazon.com/compliance/iso-27001-faqs/.

ISO 27017

ISO 27017 é o mais novo código de boas práticas divulgado pela Organização Internacional de Normalização (ISO). Ele fornece orientação de implementação em controles de segurança da informação que dizem respeito especificamente a serviços em nuvem.

A AWS obteve a certificação ISO 27017 do nosso Information Security Management System (ISMS - Sistema de gestão de segurança da informação) que abrange a infraestrutura, datacenters e serviços da AWS como:

- 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 (Web Application Firewall)
- Elastic Load Balancing
- VM Import/Export

É possível baixar a certificação ISO 27017 da AWS de https://d0.awsstatic.com/certifications/iso_27017_certification.pdf.

A AWS fornece informações adicionais e perguntas frequentes sobre sua conformidade com a certificação ISO 27017 em: https://aws.amazon.com/compliance/iso-27017-faqs/.

ISO 27018

A ISO 27018 é o primeiro código internacional de boas práticas que incide sobre a proteção de dados pessoais na nuvem. Ela é baseada no padrão de segurança da informação ISO 27002 e fornece orientação sobre a implementação dos controles da ISO 27002 aplicáveis à PII (Informações de Identificação Pessoal) de nuvens públicas. Ela também fornece um conjunto de controles adicionais e orientações associadas destinadas a abordar os requisitos de proteção PII de nuvem pública não abordados pelo conjunto de controle existente da ISO 27002.

A AWS obteve a certificação ISO 27018 do nosso Information Security Management System (ISMS - Sistema de gestão de segurança da informação) que abrange a infraestrutura, datacenters e serviços da AWS como:

- 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 (Web Application Firewall)
- Elastic Load Balancing
- VM Import/Export

É possível baixar a certificação ISO 27018 da AWS de https://d0.awsstatic.com/certifications/iso_27018_certification.pdf.

A AWS fornece informações adicionais e perguntas frequentes sobre sua conformidade com a certificação ISO 27018 em: https://aws.amazon.com/compliance/iso-27018-faqs/.

ITAR

A região AWS GovCloud (EUA) oferece suporte ao cumprimento dos ITAR (International Traffic in Arms Regulations) dos EUA. Como parte do gerenciamento de um abrangente programa de conformidade com o ITAR, empresas sujeitas a regulamentações de exportação do ITAR devem controlar as exportações não intencionais restringindo o acesso a dados protegidos de cidadãos americanos e restringindo a localização física dos dados ao território dos EUA. O AWS GovCloud (EUA) fornece um ambiente fisicamente localizado nos EUA no qual o acesso por parte do pessoal da AWS é limitado aos cidadãos americanos, permitindo que empresas qualificadas transmitam, processem e armazenem artigos e dados sujeitos às restrições do ITAR. O ambiente AWS GovCloud (EUA) foi auditado por um terceiro independente para validar que os controles apropriados estão em vigor para apoiar programas de conformidade de exportação do cliente para esse requisito.

MPAA

A Motion Picture Association of America (MPAA) estabeleceu um conjunto de melhores práticas para armazenar, processar e fornecer com segurança conteúdo e mídia protegida (http://www.fightfilmtheft.org/facility-security-program.html). As empresas de mídia usam essas práticas recomendadas como forma de avaliar o risco e a segurança do seu conteúdo e infraestrutura.
A AWS demonstrou alinhamento com as práticas recomendadas da MPAA e a infraestrutura da AWS é compatível com todos os controles de infraestrutura aplicáveis da MPAA. Embora a MPAA não ofereça uma "certificação", os clientes do setor de mídia podem usar a documentação da MPAA da AWS para aprimorar sua avaliação de riscos e do conteúdo do tipo MPAA na AWS.

Consulte a página principal Conformidade da MPAA na AWS para obter detalhes adicionais em: https://aws.amazon.com/compliance/mpaa/.

Certificação nível 3 da MTCS

A Segurança em nuvem multicamada (MTCS, Multi-Tier Cloud Security) é um padrão de gerenciamento de segurança operacional (SPRING SS 584:2013) da Cingapura baseado nos padrões do sistema de gerenciamento de segurança de informações (ISMS, Information Security Management System) ISO 27001/02. A avaliação de certificação nos obriga a:

- Avalie sistematicamente nossos riscos de segurança das informações, levando em conta o impacto das ameaças e vulnerabilidades na empresa
- Desenhe e implemente uma suíte abrangente de controles da segurança da informação e outras formas de gestão de risco para abordar os riscos de segurança na empresa e na arquitetura
- Adote um processo de gestão global para garantir que os controles de segurança da informação atendam às nossas necessidades de segurança da informação de forma contínua

Veja a página principal do MTCS em: https://aws.amazon.com/compliance/aws-multitiered-cloud-security-standard-certification/.

NIST

Em junho de 2015, o Instituto Nacional de Padrões e Tecnologia (NIST) lançou as diretrizes 800-171, "Diretrizes finais para proteger informações confidenciais do governo retidas por contratantes". Esta orientação é aplicável à proteção de CUI (Controlled Unclassified Information) em sistemas não federais.

A AWS já está em conformidade com estas diretrizes, e os clientes podem efetivamente cumprir a NIST 800-171 imediatamente. A NIST 800-171 descreve um subconjunto dos requisitos da NIST 800-53, uma diretriz segundo a qual a AWS já foi auditada no âmbito do programa FedRAMP. A linha de base de controle de segurança da FedRAMP Moderate é mais rigorosa que os requisitos recomendados estabelecidos no capítulo 3 da 800-171, e inclui um número significativo de controles de segurança acima e além dos exigidos aos sistemas FISMA Moderate que protegem os dados CUI. Um mapeamento detalhado está disponível na publicação especial NIST 800-171, começando na página D2 (página 37 no PDF).

PCI DSS, nível 1

A AWS tem conformidade nível 1 com o Padrão de Segurança de Dados (DSS) da Indústria de Cartões de Pagamento (PCI). Os clientes podem executar aplicações em nossa infraestrutura de tecnologia em conformidade com a PCI para armazenar, processar e transmitir informações de cartão de crédito na nuvem. Em fevereiro de 2013, o Conselho do Padrão de Segurança de Dados da PCI publicou as Diretrizes de Computação em Nuvem do DSS da PCI. Essas diretrizes fornecem aos clientes que administram um ambiente de dados de proprietários de cartões de crédito considerações para manter os controles do DSS da PCI na nuvem. A AWS incorporou as Diretrizes de Computação em Nuvem do DSS da PCI no Pacote de Conformidade com a PCI da AWS para os clientes. O Pacote de Conformidade com a PCI da AWS inclui o Atestado de Conformidade com a PCI (AoC) da AWS, que mostra que a AWS recebeu validação em relação às normas aplicáveis a um provedor de serviços de nível 1 no DSS da PCI versão 3.1 e o Resumo de Responsabilidade quanto à PCI da AWS, que explica como as responsabilidades de conformidade são compartilhadas entre a AWS e nossos clientes na nuvem.

Os seguintes serviços estão no escopo para o PCI DSS nível 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)
- A infraestrutura física subjacente (incluindo a GovCloud) e o Ambiente de Gerenciamento da AWS

O escopo de serviços e regiões mais recente para a certificação AWS PCI DSS nível 1 pode ser encontrado em: https://aws.amazon.com/compliance/pci-dss-level-1-faqs/.

SOC 1/ISAE 3402

A Amazon Web Services publica um relatório de controles de empresa de serviços 1 (SOC 1), tipo II. A auditoria para este relatório é conduzida de acordo com o AICPA (American Institute of Certified Public Accountants): AT 801 (antigo SSAE 16) e as Normas Internacionais para Contratos de Garantia nº 3402 (ISAE 3402). Esse relatório de padrão duplo destina-se a atender a uma ampla variedade de requisitos de auditoria financeira dos Estados Unidos e de órgãos internacionais de auditoria. A auditoria do relatório SOC 1 declara que os objetivos de controle da AWS foram devidamente desenvolvidos e que os controles individuais definidos para proteger os dados do cliente operam com eficácia. Este relatório é a substituição da Declaração sobre Normas de Auditoria nº 70 (SAS 70) tipo II.

Os objetivos de controle do SOC 1 da AWS são disponibilizados aqui. O próprio relatório identifica as atividades de controle que oferecem respaldo a cada um desses objetivos, bem como os resultados de auditores independentes de seus procedimentos de teste de cada controle.

Área do objetivo	Descrição do objetivo
Organização de segurança	Os controles fornecem garantias suficientes de que as políticas de segurança da informação foram implementadas e comunicadas em toda a organização.
Acesso de usuário para funcionários	Os controles fornecem garantias suficientes de que procedimentos foram estabelecidos para que contas de usuário de funcionários da Amazon sejam adicionadas, modificadas e excluídas em tempo hábil e sejam revistas periodicamente.
Segurança lógica	Os controles fornecem garantias suficientes de que políticas e mecanismos estão implementados para restringir adequadamente o acesso não autorizado interno e externo aos dados e os dados dos clientes são adequadamente separados dos outros clientes.
Manipulação segura de dados	Os controles fornecem garantias suficientes de que a manipulação de dados entre o ponto de início do cliente e um local de armazenamento da AWS seja protegida e mapeada com precisão.
Proteções de segurança física e ambiental	Os controles fornecem garantias suficientes de que o acesso aos datacenters está restrito ao pessoal autorizado, além da existência de mecanismos implementados para minimizar o efeito de problemas no funcionamento ou de desastres físicos para as instalações do datacenter.
Gerenciamento de alterações	Os controles fornecem garantias suficientes de que as alterações (incluindo emergência/não rotineiras e configuração) em recursos de TI existentes são registradas, autorizadas, testadas, aprovadas e documentadas.
Redundância, disponibilidade e integridade dos dados	Os controles fornecem garantias suficientes de que a integridade dos dados seja mantida em todas as fases, incluindo a transmissão, o armazenamento e o processamento.
Tratamento de incidentes	Os controles fornecem garantias suficientes de que os incidentes de sistema são registrados, analisados e resolvidos.

Os novos relatórios SOC 1 foram desenvolvidos com enfoque em controles em uma empresa de serviços, os quais provavelmente serão relevantes para uma auditoria de demonstrativos financeiros da entidade de um usuário. Como a base de clientes da AWS é ampla e o uso de serviços da AWS é igualmente amplo, a aplicabilidade dos controles aos demonstrativos financeiros de clientes varia conforme o cliente. Portanto, o relatório SOC 1 da AWS foi desenvolvido para abranger controles essenciais específicos que provavelmente serão necessários durante uma auditoria financeira, bem como abranger uma ampla variedade de controles gerais de TI, a fim de acomodar uma grande diversidade de uso e cenários de auditoria. Isso permite que os clientes utilizem a infraestrutura da AWS para armazenar e processar dados essenciais, incluindo os que são integrais ao processo de geração de relatórios financeiros. A AWS reavalia periodicamente a seleção desses controles para considerar feedback de clientes e uso desse importante relatório de auditoria.

O compromisso da AWS com o relatório SOC 1 é ininterrupto e daremos continuidade ao nosso processo de auditorias periódicas. O escopo do relatório SOC 1 abrange:

- 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

Além do relatório SOC 1, a AWS publica um relatório de controles de empresas de serviços 2 (SOC 2), tipo II. Semelhante ao SOC 1 na avaliação de controles, o SOC 2 é um relatório de comprovação que expande a avaliação de controles para os critérios definidos pelos princípios de serviços de confiança do American Institute of Certified Public Accountants (AICPA). Esses princípios definem os principais controles de prática relevantes para a segurança, disponibilidade, integridade de processamento, confidencialidade e privacidade aplicáveis a organizações de serviços como a AWS. O SOC 2 da AWS é uma avaliação do design e eficácia operacional de controles que atendem aos critérios para os princípios de segurança e disponibilidade definidos nos critérios de princípios de serviços de segurança do AICPA. Este relatório fornece mais transparência para a segurança e disponibilidade da AWS com base em um padrão predefinido das principais práticas do setor e demonstra ainda mais o compromisso da AWS com a proteção de dados de clientes. O escopo do relatório SOC 2 abrange os mesmos serviços incluídos no relatório SOC 1. Consulte a descrição do SOC 1 acima para verificar os serviços incluídos no escopo.

SOC 3

A AWS publica um relatório de controles de empresas de serviços 3 (SOC 3). O relatório SOC 3 é um resumo disponível publicamente do relatório SOC 2 da AWS. O relatório inclui a opinião do auditor externo da operação de controles (com base nos Princípios de Confiança de Segurança do AICPA incluídos no relatório SOC 2), a declaração do gerenciamento da AWS em relação à efetividade dos controles e uma visão geral da infraestrutura e serviços da AWS. O relatório SOC 3 da AWS inclui todos os datacenters da AWS em todo o mundo que dão suporte a serviços no escopo. Este é um excelente recurso para os clientes validarem que a AWS obteve garantia de um auditor externo sem passar pelo processo de solicitação de um relatório SOC 2. O escopo do relatório SOC 3 abrange os mesmos serviços incluídos no relatório SOC 1. Consulte a descrição do SOC 1 acima para verificar os serviços incluídos no escopo. Veja o relatório SOC 3 da AWS aqui.

Outras fontes de leitura

Para obter informações adicionais, consulte estas fontes:

- Visão geral dos riscos e da conformidade da AWS
- Respostas da AWS para as principais questões de conformidade
- Questionário da iniciativa de avaliação de consenso da CSA

Revisões do documento

Data	Descrição
Janeiro de 2017	Migração para novo modelo
Janeiro de 2016	Primeira publicação