# Respostas da AWS para as principais questões de conformidade

*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

Principais questões e respostas de conformidade 1

Outras fontes de leitura 9

Revisões do documento 9

# Resumo

Este documento aborda questões comuns de conformidade de computação em nuvem à medida que se relacionam à AWS. As respostas a elas podem ser de interesse ao se avaliar e operar em um ambiente de computação em nuvem e pode auxiliar os esforços de gerenciamento de controle de clientes da AWS.

# Principais questões e respostas de conformidade

| Categoria | Pergunta sobre computação em nuvem | Informações sobre a AWS |
|---|---|---|
| **Propriedade de controle** | Quem detém os controles para a infraestrutura implantada na nuvem? | Para a parte implementada na AWS, a AWS controla os componentes físicos dessa tecnologia. O cliente possui e controla todo o resto, incluindo o controle sobre pontos de conexão e transmissões. Para ajudar os clientes a compreenderem melhor os controles que temos em vigor e como efetivamente eles operam, publicamos um relatório SOC 1 tipo II com controles definidos em torno do EC2, do S3 e da VPC, bem como controles de segurança física detalhada e controles ambientais. Esses controles são definidos em um alto nível de especificidade, que deve atender a maioria das necessidades do cliente. Os clientes da AWS que assinaram um acordo de confidencialidade com a AWS podem solicitar uma cópia do relatório SOC 1 tipo II. |
| **TI de auditoria** | Como pode ser executada a auditoria do provedor de nuvem? | A auditoria da maioria das camadas e controles acima dos controles físicos permanece responsabilidade do cliente. A definição de controles lógicos e físicos definidos pela AWS é documentada no relatório SOC 1 tipo II, e o relatório está disponível para análise por equipes de auditoria e conformidade. A certificação AWS ISO 27001 e outras também estão disponíveis para que auditores analisem. |
| **Conformidade com o Sarbanes-Oxley** | Como a conformidade com o SOX é alcançada quando os sistemas no escopo são implantados no ambiente do provedor de nuvem? | Se um cliente processa informações financeiras na nuvem da AWS, as contas do cliente podem determinar que alguns sistemas da AWS entram no escopo para os requisitos da Sarbanes-Oxley (SOX). Os auditores dos clientes devem fazer sua própria determinação sobre a aplicabilidade da SOX. Como a maioria dos controles de acesso lógico é gerenciada pelo cliente, o cliente está mais bem posicionado para determinar se as suas atividades de controle atendem às normas pertinentes. Se auditores da SOX solicitarem informações específicas sobre controles físicos da AWS, eles podem consultar o relatório SOC 1 tipo II da AWS que detalha os controles fornecidos pela AWS. |

| Categoria | Pergunta sobre computação em nuvem | Informações sobre a AWS |
|---|---|---|
| **Conformidade com o HIPAA** | É possível atender aos requisitos de conformidade com o HIPAA enquanto os sistemas estiverem implantados no ambiente do provedor de nuvem? | Os requisitos da HIPAA se aplicam ao cliente AWS e são controlados por ele. A plataforma da AWS permite a implantação de soluções que atendem aos requisitos de certificação específicos do setor, como HIPAA. Os clientes podem usar os serviços da AWS para manter um nível de segurança que seja equivalente ou superior aos necessários para proteger registros eletrônicos de saúde. Os clientes têm criado aplicações na área de saúde em conformidade com as Regras de Privacidade e Segurança da HIPAA na AWS. A AWS fornece informações adicionais sobre a conformidade com o HIPAA em seu site, incluindo um whitepaper sobre este tópico. |
| **Conformidade com a GLBA** | É possível atender aos requisitos da certificação GLBA enquanto os sistemas estiverem implantados no ambiente do provedor de nuvem? | Os requisitos da GLBA se aplicam ao cliente da AWS e são controlados por ele. A AWS fornece meios para que os clientes protejam dados, gerenciem permissões e construam aplicações compatíveis com a GLBA na infraestrutura da AWS. Se o cliente requer garantia específica de que os controles físicos de segurança estão operando eficazmente, ele pode consultar o relatório AWS SOC 1 tipo II conforme pertinente. |
| **Conformidade com a regulamentação federal** | É possível que um órgão do governo dos EUA esteja em conformidade com os regulamentos de segurança e privacidade enquanto os sistemas estiverem implantados no ambiente do provedor da nuvem? | Os órgãos federais dos EUA podem estar em conformidade com determinado número de padrões de conformidade, incluindo o Federal Information Security Management Act (FISMA – Lei de administração de segurança de informações federais) de 2002, Federal Risk and Authorization Management Program (FedRAMP – Programa de administração de autorizações e riscos federais), a publicação 140-2 do Federal Information Processing Standard (FIPS – Padrão de processamento de informações) e o International Traffic in Arms Regulations (ITAR – Tráfego internacional em regulamentos de armas). A conformidade com outras leis e estatutos também pode ser acomodada dependendo dos requisitos estabelecidos na legislação aplicável. |

| Categoria | Pergunta sobre computação em nuvem | Informações sobre a AWS |
|---|---|---|
| **Local dos dados** | Onde residem os dados do cliente? | Os clientes da AWS determinam a região física em que seus dados e servidores estarão localizados. A replicação de dados para objetos de dados S3 é feita dentro do cluster regional em que os dados são armazenados e não são replicados para outros clusters de datacenters em outras regiões. Os clientes da AWS determinam a região física em que seus dados e servidores estarão localizados. A AWS não moverá o conteúdo de clientes das regiões selecionadas sem notificá-los, exceto se necessário para cumprir a legislação ou atender a solicitações de entidades governamentais. Para obter uma lista completa das regiões, consulte aws.amazon.com/about-aws/global-infrastructure. |
| **E-Discovery** | O provedor de nuvem atende às necessidades do cliente para atender aos procedimentos e requisitos de localização de dados eletrônicos? | A AWS fornece infraestrutura e os clientes gerenciam todo o resto, incluindo o sistema operacional, a configuração de rede e as aplicações instaladas. Os clientes são responsáveis por responder adequadamente aos procedimentos legais envolvendo a identificação, coleta, processamento, análise e produção de documentos eletrônicos que armazenam ou processam usando a AWS. Mediante solicitação, a AWS pode trabalhar com os clientes que precisem de auxílio da AWS em processos judiciais. |
| **Tours de datacenter** | O provedor de nuvem permite tours de clientes pelos datacenters? | Não. Devido ao fato de que nossos datacenters hospedam vários clientes, a AWS não permite tours de clientes pelos datacenters, visto que isso expõe um vasto número de clientes ao acesso físico de terceiros. Para atender a essa necessidade de cliente, um auditor independente e competente valida a presença e o funcionamento dos controles como parte do nosso relatório SOC 1 tipo II. Essa validação de terceiros amplamente aceita oferece aos clientes a perspectiva independente da eficácia dos controles em vigor. Os clientes da AWS que assinaram um acordo de confidencialidade com a AWS podem solicitar uma cópia do relatório SOC 1 tipo II. Revisões independentes sobre a segurança física do datacenter também são parte da auditoria ISO 27001, da avaliação PCI, da auditoria ITAR e dos programas de teste do FedRAMP$^{sm}$. |

| Categoria | Pergunta sobre computação em nuvem | Informações sobre a AWS |
|---|---|---|
| **Acesso de terceiros** | Terceiros têm permissão para acessar os datacenters do provedor de nuvem? | A AWS mantém um controle restrito de acesso aos datacenters, mesmo para funcionários internos. Não é concedido acesso de terceiros aos datacenters da AWS, exceto quando explicitamente aprovado pelo gerente responsável do datacenter da AWS, conforme as políticas de acesso da AWS. Consulte o relatório SOC 1 tipo II para conhecer os controles específicos relacionados ao acesso físico, à autorização de acesso a datacenters e a outros controles relacionados. |
| **Ações privilegiadas** | As ações privilegiadas são monitoradas e controladas? | Os controles implementados limitam o acesso a sistemas e dados, fornecendo acesso restrito e monitorado. Além disso, por padrão, os dados do cliente e as instâncias do servidor são logicamente isolados de outros clientes.<br>O controle de acesso de usuários privilegiados é analisado por um auditor independente durante as auditorias AWS SOC 1, ISO 27001, PCI, ITAR e FedRAMP[sm]. |
| **Acesso privilegiado** | O provedor da nuvem analisa a ameaça do acesso privilegiado inadequado a dados e aplicações de clientes? | A AWS fornece controles específicos SOC 1 para abordar a ameaça de acesso privilegiado inadequado, a certificação pública e as iniciativas de conformidade discutidas neste documento, na seção de acesso privilegiado. Todas as certificações e declarações de terceiros avaliam o acesso lógico e os controles preventivo e de detecção. Além disso, as avaliações periódicas de riscos concentram-se em como o acesso privilegiado é controlado e monitorado. |
| **Multilocação** | A segregação do cliente é implementada com segurança? | O ambiente da AWS é um ambiente multilocatário e virtualizado. A AWS implementou processos de gerenciamento de segurança, controles do PCI e outros controles de segurança projetados para isolar os clientes uns dos outros. Os sistemas da AWS são projetados para impedir que os clientes acessem hosts físicos ou instâncias não atribuídas a eles por filtragem através do software de virtualização. Essa arquitetura foi validada por um Qualified Security Assessor (QSA) independente do PCI e foi determinada para estar em conformidade com todos os requisitos do PCI DSS, versão 3.1, publicado em abril de 2015.<br>**Nota**: a AWS também tem opções de locação única. Instâncias dedicadas são instâncias do Amazon EC2 iniciadas da sua Amazon Virtual Private Cloud (Amazon VPC) que executam |

| Categoria | Pergunta sobre computação em nuvem | Informações sobre a AWS |
|---|---|---|
| | | o hardware dedicado a um único cliente. Instâncias dedicadas permitem que você tire total proveito dos benefícios do Amazon VPC e da Nuvem AWS enquanto isola as suas instâncias de computação do Amazon EC2 no nível de hardware. |
| **Vulnerabilidades do hypervisor** | O provedor de nuvem abordou as vulnerabilidades conhecidas do hypervisor? | O Amazon EC2 atualmente utiliza uma versão altamente personalizada do hypervisor Xen. O hypervisor é regularmente avaliado para verificar vulnerabilidades novas e existentes e vetores de ataque por equipes de penetração interna e externa e é bem adequado para manter um rígido isolamento entre máquinas virtuais convidadas. O hypervisor AWS Xen é regularmente avaliado por auditores independentes durante avaliações e auditorias. Consulte o whitepaper de segurança da AWS para obter mais informações sobre o isolamento de hypervisores e instâncias. |
| **Gerenciamento de vulnera-bilidades** | Os sistemas são corrigidos adequadamente? | A AWS é responsável por corrigir sistemas que oferecem suporte ao fornecimento de serviços a clientes, como o hypervisor e os serviços de rede. Isso é feito como exigido pela política da AWS e em conformidade com o ISO 27001, NIST e os requisitos do PCI. Os clientes controlam seus próprios sistemas operacionais, softwares e aplicações convidados e, por isso, são responsáveis por corrigir seus próprios sistemas. |
| **Criptografia** | Os serviços fornecidos oferecem suporte a criptografia? | Sim. A AWS permite que os clientes usem seus próprios mecanismos de criptografia para quase todos os serviços, incluindo S3, EBS, SimpleDB e EC2. Os túneis IPSec para a VPC também são criptografados. O Amazon S3 também oferece criptografia no servidor como uma opção para os clientes. Os clientes também podem usar tecnologias de criptografia de terceiros. Consulte o whitepaper de segurança da AWS para obter mais informações. |
| **Propriedade de dados** | Quais são os direitos do provedor de nuvem sobre os dados do cliente? | Os clientes da AWS mantêm o controle e a propriedade sobre os seus dados. A AWS não mede esforços para proteger a privacidade de seus clientes e se mantém atenta ao determinar as solicitações legais com as quais deve estar em conformidade. A AWS não hesita em contestar ordens legais se acreditar que elas sejam infundadas ou não possuam embasamento sólido. |

| Categoria | Pergunta sobre computação em nuvem | Informações sobre a AWS |
|---|---|---|
| **Isolamento de dados** | O provedor de nuvem isola adequadamente dados de clientes? | Todos os dados armazenados pela AWS em nome dos clientes têm recursos sólidos de segurança e controle de isolamento de grupos de usuários. O Amazon S3 fornece controles de acesso de dados avançados. Consulte o whitepaper de segurança da AWS para obter mais informações sobre a segurança de serviços de dados específicos. |
| **Serviços compostos** | O provedor de nuvem fornece seus serviços em nuvem em conjunto com os serviços de outros provedores? | A AWS não utiliza nenhum provedor de terceiros para fornecer serviços a clientes. |
| **Controles físicos e ambientais** | Estes controles são operados por um provedor em nuvem especificado? | Sim. Estes são descritos especificamente no relatório SOC 1, tipo II. Além disso, outros suportes de certificações da AWS, como o ISO 27001 e o FedRAMP[sm], requerem controles de melhores práticas físicas e ambientais. |
| **Proteção do lado do cliente** | O provedor de nuvem permite que os clientes protejam e gerenciem o acesso de aplicativos clientes em computadores e dispositivos móveis, por exemplo? | Sim. A AWS permite aos clientes gerenciar os aplicativos móveis e clientes de acordo com suas próprias necessidades. |
| **Segurança do servidor** | O provedor de nuvem permite que clientes protejam seus servidores virtuais? | Sim. A AWS permite que os clientes implementem sua própria arquitetura de segurança. Consulte o whitepaper de segurança da AWS para obter mais detalhes sobre a segurança do servidor e da rede. |
| **Identity and Access Management** | O serviço inclui funções do IAM? | A AWS tem um conjunto de ofertas de gerenciamento de identidades e acesso, que permite aos clientes gerenciar identidades de usuários, atribuir credenciais de segurança, organizar usuários em grupos e gerenciar permissões do usuário de uma forma centralizada. Consulte o site da AWS para obter mais informações. |
| **Paralizações de manutenção programadas** | O provedor especifica quando os sistemas serão paralisados para manutenção? | A AWS não exige que os sistemas sejam paralisados para executar a manutenção regular e aplicação de correções de sistema. A manutenção da AWS e a aplicação de correções de sistema geralmente não afetam os clientes. A manutenção das instâncias em si é controlada pelo cliente. |

| Categoria | Pergunta sobre computação em nuvem | Informações sobre a AWS |
|---|---|---|
| **Função para fazer escalonamento** | O provedor da nuvem permite a clientes fazer escalonamento de conteúdo além do que permite o contrato original? | A nuvem da AWS é distribuída, altamente segura e flexível, dando aos clientes enorme potencial de escalabilidade. Os clientes podem fazer escalonamento de seus recursos para mais ou para menos, pagando apenas pelo que usam. |
| **Disponibilidade de serviços** | O provedor se compromete com um nível elevado de disponibilidade? | A AWS se compromete com altos níveis de disponibilidade em seus contratos de níveis de serviço (SLA). Por exemplo, o Amazon EC2 compromete-se com a porcentagem de tempo de atividade anual de pelo menos 99,95% durante o ano de serviço. O Amazon S3 se compromete com uma porcentagem de tempo de atividade mensal de pelo menos 99,9%. São fornecidos créditos de serviço caso essas métricas de disponibilidade não sejam cumpridas. |
| **Ataques DDoS** | Como o provedor protege seu serviço contra ataques DDoS? | A rede da AWS fornece proteção significativa contra problemas de segurança de rede tradicional e o cliente pode implementar mais proteção. Consulte o whitepaper de segurança da AWS para obter mais informações sobre esse tópico, incluindo uma discussão sobre ataques DDoS. |
| **Portabilidade de dados** | Os dados armazenados em um provedor de serviço podem ser exportados por solicitação do cliente? | A AWS permite que os clientes movam os dados conforme necessário e desativem o armazenamento da AWS. O serviço AWS Import/Export para o S3 acelera a entrada e a saída de grandes volumes de dados da AWS usando dispositivos portáteis de armazenamento para transporte. |
| **Continuidade comercial da prestadora de serviços** | A prestadora de serviços opera um programa de continuidade comercial? | A AWS executa um programa de continuidade de negócios. São fornecidas informações detalhadas no whitepaper de segurança da AWS. |
| **Continuidade comercial do cliente** | A prestadora de serviços permite que clientes implementem um plano de continuidade comercial? | A AWS fornece aos clientes a opção de implementar um plano de continuidade consistente, incluindo a utilização de backups frequentes do servidor, a replicação de redundância de dados e arquiteturas de implantação da zona de disponibilidade/multirregião. |

| Categoria | Pergunta sobre computação em nuvem | Informações sobre a AWS |
|---|---|---|
| **Durabilidade de dados** | O serviço especifica a durabilidade dos dados? | O Amazon S3 fornece uma infraestrutura de armazenamento altamente durável. Os objetos são armazenados de forma redundante em vários dispositivos em diversas instalações em uma região do Amazon S3. Uma vez armazenados, o Amazon S3 mantém a durabilidade dos objetos ao detectar e reparar rapidamente qualquer redundância perdida. O Amazon S3 também verifica regularmente a integridade dos dados armazenados usando somas de verificação. Se uma corrupção for detectada, ela será reparada usando dados redundantes. Os dados armazenados no S3 são projetados para fornecer disponibilidade de 99,99% de objetos e durabilidade de 99,999999999% ao longo de um determinado ano. |
| **Backups** | O serviço fornece backups em unidades de fita? | A AWS permite que clientes executem seus backups usando seu próprio provedor de serviço de backup em unidades de fita. No entanto, um backup em fita não é um serviço prestado pela AWS. O serviço Amazon S3 é projetado para conduzir a probabilidade de perda de dados para perto de zero por cento e a durabilidade equivalente das cópias multissite de objetos de dados é conseguida através de redundância de armazenamento de dados. Para obter informações sobre durabilidade e redundância de dados, consulte o website da AWS. |
| **Aumentos de preço** | A prestadora de serviços aumenta os preços de forma inesperada? | A AWS tem um histórico de redução frequente de preços à medida que o custo para fornecer esses serviços decresce ao longo do tempo. A AWS tem reduzido preços consistentemente ao longo dos últimos anos. |
| **Sustentabilidade** | A empresa prestadora de serviço tem potencial de sustentabilidade de longo prazo? | A AWS é um provedor líder de nuvem e é uma estratégia de negócios de longo prazo da Amazon.com. A AWS tem um potencial muito elevado de sustentabilidade a longo prazo. |

# Outras fontes de leitura

Para obter informações adicionais, consulte estas fontes:

- Visão geral dos riscos e da conformidade da AWS
- Certificações, programas, relatórios e atestados de terceiros da AWS
- 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 |