Amazon Web Services: programa de conformidade e gerenciamento de riscos

Julho de 2012

(Consulte o http://aws.amazon.com/pt/security para obter a versão mais recente deste documento.)

Este documento tem a intenção de fornecer informações para auxiliar os clientes da AWS a integrar a AWS à estrutura de controle existente, que oferece suporte ao seu ambiente de TI. Este documento inclui uma abordagem básica para avaliar controles da AWS e para fornecer informações que ajudem os clientes na integração de ambientes de controle. Este documento também aborda informações específicas da AWS sobre questões gerais de conformidade de computação em nuvem.

Este documento contém os seguintes tópicos:

Visão geral do programa de conformidade e gerenciamento de riscos

Visto que a AWS e seus clientes compartilham o controle sobre o ambiente de TI, ambas as partes têm a responsabilidade de gerenciar o ambiente de TI. A participação da AWS nesta responsabilidade compartilhada inclui fornecer seus serviços em uma plataforma altamente segura e controlada, bem como disponibilizar uma grande variedade de recursos de segurança que pode ser usada por seus clientes. A responsabilidade dos clientes inclui a configuração de seus ambientes de TI de forma segura e controlada para os seus propósitos. Mesmo se os clientes não comunicarem o seu uso e as suas configurações para a AWS, a AWS comunica a sua segurança e o ambiente de controle relevante para os clientes. A AWS faz isso da seguinte maneira:

- Obtendo certificações do setor e declarações de terceiros independentemente do descrito neste documento.
- Publicando informações sobre as práticas de controle e segurança da AWS nos whitepapers e no conteúdo do site.
- Fornecendo certificados, relatórios e outra documentação diretamente para clientes da AWS mediante acordo de confidencialidade (ou NDA, Non-Disclosure Agreement), conforme necessário.

Consulte o whitepaper de segurança da AWS, localizado em www.aws.amazon.com/pt/security, para obter uma descrição mais detalhada sobre a segurança da AWS. O whitepaper de segurança da AWS aborda os controles de segurança gerais e os serviços de segurança específicos da AWS.

Ambiente de responsabilidade compartilhada

Ao mover-se a infraestrutura de TI para os serviços da AWS cria-se um modelo de responsabilidade compartilhada entre o cliente e a AWS. Esse modelo compartilhado pode auxiliar a reduzir as preocupações operacionais do cliente em relação a como a AWS opera, gerencia e controla os componentes do sistema operacional do host e a camada de virtualização, incluindo a segurança física das instalações em que o serviço opera. O cliente assume a gestão e a responsabilidade pelo sistema operacional convidado (inclusive atualizações e patches de segurança), por outro software de aplicativo associado, bem como pela configuração do firewall do grupo de segurança fornecido pela AWS. Os clientes devem examinar cuidadosamente os serviços que escolherem, bem como as suas respectivas responsabilidades que variam de acordo com os serviços utilizados, a integração desses serviços no seu ambiente de TI e as leis e regulamentos aplicáveis. Os clientes são capazes de aumentar a segurança e/ou atender aos seus mais rigorosos requisitos de conformidade ao utilizar tecnologia como criptografia e gerenciamento de chaves, detecção/prevenção de invasões e firewalls baseados em host. A natureza dessa responsabilidade compartilhada também fornece a flexibilidade e o controle do cliente, que permitem a implementação de soluções que atendam aos requisitos de certificação específicos do setor.

Esse modelo de responsabilidade compartilhada entre o cliente e a AWS também se estende aos controles de TI. Assim como a responsabilidade para operar o ambiente de TI é compartilhada entre a AWS e os seus clientes, isso ocorre com o gerenciamento, com a operação e com a verificação de controles compartilhados de TI. A AWS pode auxiliar a diminuir a preocupação do cliente em relação aos controles operacionais gerenciando os controles associados à infraestrutura física implementada no ambiente da AWS que anteriormente tenha sido gerenciado pelo cliente. Já que cada cliente é implementado de forma diferente na AWS, os clientes podem tirar proveito da mudança de gerenciamento de determinado controle de TI para a AWS, que resulta em um (novo) ambiente de controle distribuído. Os clientes podem então utilizar a documentação de conformidade e controle da AWS disponível (descrita na seção "Declarações de terceiros e certificações da AWS" deste documento) para realizar procedimentos de avaliação e verificação de controle, conforme necessário.

A próxima seção fornece uma abordagem sobre como os clientes da AWS podem avaliar e validar eficazmente o seu ambiente de controle distribuído.

Controle rígido de conformidade

Como sempre, solicita-se que os clientes da AWS sigam mantendo uma gestão adequada ao longo de todo o ambiente de controle de TI, independentemente de como a TI é implementada. As principais práticas incluem uma compreensão dos objetivos de conformidade e requisitos exigidos (a partir de fontes relevantes), a criação de um ambiente de controle que atenda a esses requisitos e objetivos, uma compreensão de validação necessária com base na tolerância ao risco da organização e a verificação da eficácia operacional do ambiente de controle da organização. A implementação na nuvem da AWS oferece às empresas diferentes opções para aplicar diversos tipos de controles e vários métodos de verificação.

Gestão e conformidade rígida do cliente podem incluir a seguinte abordagem básica:

1. Revise as informações disponíveis na AWS juntamente com outras informações para entender o máximo possível sobre o ambiente de TI e, em seguida, documente todos os requisitos de conformidade.
2. Projete e implemente os objetivos de controle para atender aos requisitos de conformidade corporativa.
3. Identifique e documente controles pertencentes a terceiros.
4. Verifique se todos os objetivos de controle são atendidos e todos os controles principais foram projetados com eficiência e se apresentam bom funcionamento.

Abordar a gestão de conformidade dessa forma ajudará as empresas a obterem uma melhor compreensão do ambiente de controle e ajudará a delinear claramente as atividades de verificação a serem executadas.

Avaliação e integração dos controles da AWS

A AWS fornece aos seus clientes uma ampla variedade de informações relacionadas ao seu ambiente de controle de TI por meio de whitepapers, relatórios, certificações e declarações de terceiros. Esta documentação ajuda os clientes a compreenderem os controles vigentes relevantes aos serviços da AWS que eles usam e como esses controles foram validados. Essas informações ajudam os clientes a prestarem contas e a validarem se os controles no seu ambiente de TI estendido estão operando de modo eficaz.

Tradicionalmente, o projeto e a eficácia operacional de objetivos de controle e controles são validados por auditores internos e/ou externos através de passo a passo do processo e de avaliação de evidências. A observação/verificação direta — pelo cliente ou auditor externo do cliente — é geralmente realizada para validar controles. No caso de utilização de prestadores de serviços, tais como a AWS, solicita-se que as empresas avaliem declarações de terceiros e certificações, a fim de obter uma garantia razoável do projeto e eficácia operacional do objetivo de controle e dos controles. Como resultado, embora os controles essenciais do cliente possam ser gerenciados pela AWS, o ambiente de controle ainda pode ser uma estrutura unificada, onde todos os controles são considerados e verificados como operacionais com eficácia. Declarações de terceiros e certificações da AWS podem não apenas fornecer um nível mais alto de validação do ambiente de controle, mas podem também eximir os clientes do requisito de terem de realizar determinados trabalhos de validação para seu ambiente de TI na nuvem da AWS.

A AWS fornece informações de controle de TI aos clientes de duas maneiras:

1. **Definição de controle específico.** Os clientes da AWS podem identificar os principais controles gerenciados pela AWS. Controles essenciais são críticos para o ambiente de controle do cliente e exigem uma declaração externa da eficácia operacional desses controles essenciais para que possa estar em ordem com os requisitos de conformidade — tais como a auditoria financeira anual. Para esse fim, a AWS publica uma ampla variedade de controles de TI específicos em seu relatório de controles organizacionais de serviço 1 (SOC 1), tipo II. O relatório SOC 1, anteriormente o relatório de declaração sobre as normas de auditoria (SAS) n° 70, empresas de serviços, e comumente referido como o relatório de declaração sobre normas para comprovação de contratos n° 16 (SSAE 16), é um padrão amplamente reconhecido de auditoria desenvolvido pelo American Institute of Certified Public Accountants (AICPA). A auditoria SOC 1 é uma auditoria aprofundada do projeto e da eficácia operacional de atividades de controle e objetivos de controle definidos da AWS (que incluem objetivos de controle e atividades de controle sobre a parte da infraestrutura que a AWS gerencia). O "tipo II" refere-se ao fato de que cada um dos controles descritos no relatório não é somente avaliado para adequação do projeto, mas também é testado em relação à eficácia operacional pelo auditor externo. Em virtude da independência e competência do auditor externo da AWS, os controles identificados no relatório devem fornecer aos clientes um elevado nível de confiança no ambiente de controle da AWS. Os controles da AWS podem ser considerados desenvolvidos e operacionais com eficácia para muitos fins de conformidade, incluindo auditorias de demonstrativos financeiros, de acordo com a seção 404 da Sarbanes-Oxley (SOX). A utilização de relatórios SOC 1, tipo II, geralmente também é permitida por outros órgãos externos de certificação (por exemplo, auditores do ISO 27001 podem solicitar um relatório SOC 1, tipo II, para concluir suas avaliações para os clientes).

Outras atividades de controle específicas relacionam-se à conformidade com a Federal Information Security Management Act (FISMA) e Payment Card Industry (setor de cartões de pagamento, PCI) da AWS. Como apresentado a seguir, a AWS está em conformidade com os padrões da FISMA, nível moderado, e com o padrão de segurança de dados do PCI. Ospadrões do PCI e da FISMA são muito prescritivos e requerem uma validação independente de que a AWS está aderindo aos padrões publicados.

2. **Conformidade padrão de controle geral.** Se um cliente da AWS requer que um amplo conjunto de objetivos de controle seja atendido, uma avaliação das certificações do setor da AWS pode ser realizada. Com a certificação ISO 27001 da AWS, a AWS comprova estar em conformidade com um amplo e abrangente padrão de segurança e comprova seguir as práticas recomendadas de segurança para manter um ambiente seguro. Com o padrão de segurança de dados do PCI (PCI DSS, Payment Card Industry Data Security Standard), a AWS está em conformidade com um conjunto de controles importantes para as empresas que lidam com informações de cartão de crédito. Com a conformidade da AWS com os padrões da FISMA, a AWS comprova sua conformidade com uma ampla variedade de controles específicos exigidos pelas agências governamentais americanas.
   A conformidade com esses padrões gerais disponibiliza aos clientes informações detalhadas sobre a natureza abrangente dos controles e processos de segurança em vigor e pode ser considerada ao gerenciar a conformidade.

Declarações de terceiros e certificações da AWS são discutidas em mais detalhes posteriormente neste documento.

Programa de conformidade e gerenciamento de riscos da AWS

A AWS fornece informações sobre seu programa de conformidade e gerenciamento de riscos para permitir que os clientes incorporem controles da AWS em sua estrutura de gestão. Essas informações podem ajudar os clientes a documentar uma estrutura de gestão e de controle completa com a AWS incluída como uma parte importante dessa estrutura.

Gerenciamento de riscos

A gerência da AWS desenvolveu um plano estratégico de negócios, que inclui a identificação de riscos e a implementação de controles para reduzir ou gerenciar riscos. A gerência da AWS avalia o plano estratégico de negócios pelo menos duas vezes por ano. Esse processo requer gerenciamento para identificar riscos em suas áreas de responsabilidade, bem como para implementar medidas adequadas projetadas para solucionar esses riscos.

Além disso, o ambiente de controle da AWS está sujeito a várias avaliações internas e externas de riscos. As equipes de segurança e conformidade da AWS estabeleceram políticas e uma estrutura de segurança da informação com base na estrutura dos COBIT (Control Objectives for Information and related Technology, Objetivos de controle para informações e tecnologia relacionada) e integraram com eficácia a estrutura certificável por ISO 27001, com base em controles do ISO 27002, na PCI DSS e na Publicação 800-53, rev. 3, do NIST (National Institute of Standards and Technology, Instituto nacional de padrões e tecnologia) (Controles de segurança recomendados para sistemas de informações federais). A AWS mantém a política de segurança, oferece treinamento de segurança para os funcionários e realiza revisões de segurança do aplicativo. Essas avaliações verificam a confidencialidade, a integridade e a disponibilidade de dados, bem como a conformidade com a política de segurança da informação.

A segurança da AWS examina regularmente todos os endereços IP de endpoint, de serviço voltado à Internet, quanto à existência de vulnerabilidades (essas verificações não incluem instâncias de clientes). A segurança da AWS notificará as partes adequadas para solucionar quaisquer vulnerabilidades identificadas. Além disso, avaliações de ameaça de vulnerabilidade externa são realizadas regularmente por empresas de segurança independentes. As conclusões e recomendações resultantes dessas avaliações são categorizadas e entregues à liderança da AWS. Essas verificações são feitas para avaliar a saúde e a viabilidade da infraestrutura subjacente da AWS e não se destinam a substituir as verificações de vulnerabilidade do cliente necessárias para atender aos seus requisitos de conformidade específicos. Os clientes podem solicitar permissão para conduzir pesquisas de sua infraestrutura em nuvem, somente se essas se limitarem a instâncias do cliente e não violarem a política de uso aceitável da AWS. A prévia aprovação para esses tipos de verificações pode ser iniciada ao se enviar uma solicitação através do formulário AWS Vulnerability/Penetration Testing Request (Solicitação de teste de penetração/vulnerabilidade da AWS).

Ambiente de controle da AWS

A AWS gerencia um ambiente de controle abrangente que inclui políticas, processos e atividades de controle que utilizam diversos aspectos do ambiente de controle geral da Amazon. Esse ambiente de controle está em vigor para a entrega segura de ofertas de serviços da AWS. O ambiente de controle coletivo abrange as pessoas, os processos e a tecnologia necessários para estabelecer e manter um ambiente que ofereça suporte à eficácia operacional da estrutura de controle da AWS. A AWS integrou controles específicos de nuvem aplicáveis identificados pelos principais órgãos do setor de computação em nuvem na estrutura de controle da AWS. A AWS continua acompanhando esses grupos de setor quanto a ideias sobre como as práticas de liderança podem ser implementadas para melhor atender aos clientes no gerenciamento de seu ambiente de controle.

O ambiente de controle na Amazon inicia no mais alto nível da empresa. As liderança executiva e sênior desempenham um papel importante no estabelecimento de valores fundamentais e objetivo da empresa. Cada funcionário recebe o código de ética conduta nos negócios da empresa, bem como realiza treinamento periódico. As auditorias de conformidade são realizadas para que os funcionários entendam e sigam as políticas estabelecidas.

A estrutura organizacional da AWS fornece uma estrutura para planejar, executar e controlar as operações de negócios. A estrutura organizacional atribui funções e responsabilidades para fornecer uma equipe adequada, eficiência das operações e a diferenciação de direitos. A gerência também estabeleceu autoridade e linhas apropriadas de subordinação para a equipe principal. Estão incluídos como parte dos processos de verificação para contratação da empresa a educação, o emprego anterior e, em alguns casos, a verificação de antecedentes conforme permitido pela legislação e por regulamentos. A empresa segue um processo estruturado de ambientação para familiarizar novos funcionários com as ferramentas, processos, sistemas, políticas e procedimentos da Amazon.

Segurança da informação

A AWS implementou um programa formal de segurança da informação, o qual foi desenvolvido para proteger a confidencialidade, integridade e disponibilidade de sistemas e dados dos clientes. A AWS publica um whitepaper de segurança que está disponível no site público, que aborda como a AWS pode ajudar os clientes a proteger seus dados.

Declarações de terceiros e certificações da AWS

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

SOC 1/SSAE 16/ISAE 3402

A Amazon Web Services agora publica um relatório de controles organizacionais de serviço 1 (SOC 1), tipo II. A auditoria para esse relatório é realizada de acordo com a declaração sobre normas para comprovação de contratos nº 16 (SSAE 16) e as Normas internacionais para contratos de garantia nº 3402 (ISAE 3402), normas profissionais. 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, bem como que os controles individuais definidos para proteger os dados do cliente funcionam com eficácia. Essa auditoria é a substituição do relatório de auditoria 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.

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 da Amazon	Os controles fornecem garantias suficientes de que foram estabelecidos procedimentos para que contas de usuário da Amazon sejam adicionadas, modificadas e excluídas em tempo hábil e sejam revistas periodicamente.
Segurança lógica	Os controles fornecem garantias suficientes de que acesso não autorizado interno e externo aos dados é adequadamente restrito e o acesso aos dados dos clientes é adequadamente separado 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 para um local de armazenamento da AWS, será protegida e mapeada com precisão.
Segurança física e proteções ambientais	Os controles fornecem garantias suficientes de que o acesso físico aos prédios de operações e aos datacenters está restrito ao pessoal autorizado, bem como que há procedimentos para minimizar o efeito de problemas no funcionamento ou desastres físicos para computadores e para 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 de dados	Os controles fornecem garantias suficientes de que a integridade dos dados é 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 de SOC 1 foram desenvolvidos para foco 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 aplicação de controles a 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 continuaremos como o nosso processo de auditorias periódicas. O escopo do relatório SOC 1 abrange o Amazon Elastic Compute Cloud (EC2), o Amazon Simple Storage Service (S3), o Amazon Virtual Private Cloud (VPC), o Amazon Elastic Block Store (EBS), o Amazon Relational Database Service (RDS), o Amazon DynamoDB, o Amazon Direct Connect, o Amazon VM Import, o Amazon Storage Gateway e a infraestrutura na qual eles são executados para todas as regiões no mundo inteiro.

FISMA, nível moderado

A AWS permite que clientes governamentais dos EUA obtenham e mantenham conformidade com a Lei Federal de Gestão de Segurança da Informação (FISMA) dos EUA. A FISMA exige que as agências federais desenvolvam, documentem e implementem um sistema de segurança da informação para seus dados e infraestrutura com base no padrão da Publicação especial 800-53, revisão 3, do Instituto nacional de padrões e tecnologia (NIST). A acreditação e a autorização da FISMA, em nível moderado, exigem que a AWS implemente e opere um extenso conjunto de controles e processos de segurança. Isso inclui documentar os processos de gerenciamento, operacionais e técnicos usados para proteger a infraestrutura física e virtual, bem como a auditoria de terceiros de processos estabelecidos e controles. A AWS recebeu uma autorização FISMA, de nível moderado, por três anos para a Infraestrutura como Serviço da Administração de Serviços Gerais. Além disso, as ofertas de terceiros incorporadas na AWS também receberam ATOs da FISMA, em nível moderado, de agências governamentais.

PCI DSS, nível 1

A AWS satisfaz os requisitos do PCI DSS para provedores de hospedagem compartilhada. A AWS também tem sido validada com êxito contra normas aplicáveis a um provedor de serviço de nível 1 com o PCI DSS versão 2.0. Comerciantes e outros provedores de serviço PCI poderão usar a infraestrutura de tecnologia compatível com o PCI da AWS para armazenar, processar e transmitir as informações de cartão de crédito na nuvem, mas somente se esses clientes obtiverem conformidade com o PCI para a sua parte do ambiente compartilhado. Essa validação de conformidade inclui o Amazon EC2, o Amazon S3, o Amazon EBS, o Amazon VPC, o Amazon RDS, o Amazon Elastic Load Balancing (ELB), o Amazon Identity and Access Management (IAM) e a infraestrutura na qual eles são executados para todas as regiões no mundo inteiro. A AWS fornece informações adicionais e perguntas frequentes sobre sua conformidade com o PCI em seu site e trabalha com clientes diretamente na preparação e implementação de um ambiente de titular de cartão em conformidade com o PCI na infraestrutura da AWS.

ISO 27001

A AWS obteve a certificação ISO 27001 do nosso sistema de gestão de segurança da informação (ISMS - Information Security Management System) que abrange a infraestrutura, os datacenters e os serviços da AWS, incluindo o Amazon EC2, Amazon S3 e Amazon VPC. O 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. A certificação ISO 27001 da AWS inclui todos os datacenters da AWS, em todas as regiões do mundo e a AWS estabeleceu um programa formal para manter a certificação. A AWS fornece informações adicionais e perguntas frequentes sobre sua conformidade com o ISO 27001 no seu website.

Regulamentos sobre o tráfico internacional de armas

A região AWS GovCloud (US), oferecida pela AWS, fornece suporte à conformidade com os regulamentos sobre o tráfico internacional de armas (ITAR). Como parte do gerenciamento de um abrangente programa de conformidade com os ITAR, empresas sujeitas a regulamentos de exportação dos ITAR devem controlar as exportações não intencionais ao restringir o acesso a dados protegidos de pessoas nos EUA e restringir a localização física desses dados ao território dos EUA. O AWS GovCloud (US) fornece um ambiente fisicamente localizado nos EUA no qual o acesso de colaboradores da AWS é limitado aos cidadãos dos EUA, permitindo que empresas qualificadas transmitam, processem e armazenem artigos e dados protegidos sob os ITAR. O ambiente AWS GovCloud (US) foi auditado por um terceiro independente para validar que os controles apropriados estejam em vigor para apoiar programas de conformidade de exportação do cliente para esse requisito.

FIPS 140-2

A publicação do Federal Information Processing Standard (FIPS) 140-2 é um padrão de segurança do governo dos EUA que especifica os requisitos de segurança para módulos criptográficos protegendo informações confidenciais. Para oferecer suporte a clientes com requisitos FIPS 140-2, os endpoints da VPN da Amazon Virtual Private Cloud e Load Balancers de terminação SSL no AWS GovCloud (US) operam usando o hardware validado pela FIPS 140-2. A AWS trabalha com clientes do AWS GovCloud (US) para fornecer as informações necessárias para ajudar a gerenciar a conformidade ao usar o ambiente AWS GovCloud (EUA).

Outras iniciativas de conformidade

A flexibilidade e o controle do cliente oferecido pela plataforma da AWS permitem a implantação de soluções que atendam aos requisitos de conformidade específicos do setor.

- HIPAA: os clientes criaram aplicativos na área de saúde em conformidade com as Regras de privacidade e segurança do HIPPA na AWS. A AWS fornece os controles de segurança que os clientes podem usar para ajudar a proteger registros eletrônicos de saúde. Consulte o whitepaper relacionado (link a seguir).
- CSA: a AWS concluiu o Questionário de Iniciativa de Avaliações da CSA (Cloud Security Alliance, Aliança de Segurança em Nuvem). Esse questionário publicado pela CSA fornece uma forma de consultar e documentar quais controles existem nas ofertas de Infraestrutura como Serviço da AWS. O questionário (CAIQ) fornece um conjunto de mais de 140 perguntas que um auditor de nuvem e cliente de nuvem podem querer fazer a um provedor de nuvem. Consulte o Apêndice A deste documento para verificar o Questionário de Iniciativa de Avaliações da CSA (Cloud Security Alliance, Aliança de Segurança em Nuvem) concluído pela AWS.

Principais questões de conformidade e a AWS

Esta seção aborda questões de conformidade genéricas sobre computação em nuvem especificamente para a AWS. Estes problemas comuns de conformidade relacionados podem ser de interesse ao se avaliar e operar em um ambiente de computação em nuvem e podem contribuir para os esforços de gerenciamento de controle dos clientes da AWS.

Ref	Tópico da questão de computação em nuvem	Informações sobre a AWS
1	Propriedade de dados. Quem é o proprietário de quais controles para a infraestrutura implementada em 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 sobre 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.
2	Auditoria de TI. Como é possível realizar a auditoria do provedor em nuvem?	A auditoria para a maioria das camadas e de controles acima dos controles físicos continua a ser de responsabilidade do cliente. A definição de controles lógicos e físicos definidos pela AWS é documentada no relatório SOC 1 tipo II (SSAE 16), e o relatório está disponível para análise por equipes de auditoria e conformidade. O ISO 27001 da AWS e outras certificações também estão disponíveis para análise dos auditores.
3	Conformidade com a Sarbanes-Oxley. Como estar em conformidade com a SOX se sistemas em escopo são implementados no ambiente de provedor em 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 SOX solicitarem informações específicas sobre controles físicos da AWS, eles podem fazer referência ao relatório SOC 1 tipo II da AWS que detalha os controles que a AWS fornece.
4	Conformidade com a HIPAA. É possível atender aos requisitos de conformidade com HIPAA com implementação no ambiente de provedor em 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 criaram aplicativos na área de saúde em conformidade com as Regras de privacidade e segurança da HIPPA na AWS. A AWS fornece informações adicionais sobre a conformidade da HIPAA em seu site, incluindo um whitepaper desse tema.

5	Conformidade com a GLBA. É possível atender aos requisitos de certificação da GLBA com implementação no ambiente de provedor em nuvem?	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 aplicativos compatíveis com a GLBA na infraestrutura da AWS. Se o cliente exigir garantia específica de que controles de segurança física estão operando com eficiência, eles podem fazer referência ao relatório SOC 1 tipo II da AWS conforme for apropriado.
6	Conformidade com os regulamentos federais. É possível para uma agência do governo dos Estados Unidos estar em conformidade com as normas de segurança e privacidade com implementação no ambiente de provedor em nuvem?	As agências federais dos EUA podem estar em conformidade com vários padres de conformidade, incluindo a Federal Information Security Management Act (FISMA) de 2002, a Publicação 140-2 do Federal Information Processing Standard (FIPS) e os International Traffic in Arms Regulations (ITAR). A conformidade com outras leis e estatutos também pode ser acomodada dependendo dos requisitos estabelecidos na legislação aplicável.
7	Localização dos dados. Onde ficam os dados do cliente?	Os clientes da AWS determinam a região física em que seus dados e seus 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 seus servidores estarão localizados. A AWS não moverá o conteúdo de clientes das Regiões selecionadas sem notificar o cliente, exceto se necessário para cumprir a legislação ou solicitações de entidades governamentais. A AWS atualmente oferece oito regiões: Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Norte da Califórnia), Oeste dos EUA (Oregon), GovCloud (EUA) (Oregon), UE (Irlanda), Ásia-Pacífico (Cingapura), Ásia-Pacífico (Tóquio) e América do Sul (São Paulo).
8	E-Discovery. O provedor em nuvem atende às necessidades do cliente para atender aos requisitos e aos procedimentos de detecção eletrônica?	A AWS fornece infraestrutura e os clientes gerenciam todo o resto, incluindo o sistema operacional, a configuração de rede e os aplicativos instalados. 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. Em caso de solicitação, a AWS pode trabalhar com clientes que precisem de assistência da AWS em processos judiciais.

9	Tours pelos datacenters. Os tours de clientes pelos datacenters são autorizados pelo provedor em nuvem?	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 (SSAE 16). 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. Análises independentes da segurança física do datacenter também fazem parte da auditoria ISO 27001, da avaliação do PCI, da auditoria dos ITAR e dos programas de testes da FISMA.
10	Acesso de terceiros. É permitido o acesso de terceiros aos datacenters de provedor em nuvem?	A AWS mantém um controle restrito de acesso aos datacenters, mesmo para funcionários internos. O acesso de terceiros aos datacenters da AWS não é concedido, exceto quando for explicitamente aprovado pelo gerente de datacenter da AWS responsável, conforme as políticas de acesso da AWS. Consulte o relatório SOC 1, tipo II, para controles específicos referentes ao acesso físico, à autorização de acesso ao datacenter e a outros controles relacionados.
11	Ações privilegiadas. As ações privilegiadas são monitoradas e controladas?	Os controles implementados limitam o acesso aos sistemas e aos 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. O controle de acesso de usuário privilegiado é revisto por um auditor independente durante as auditorias SOC 1, ISO 27001, PCI, ITAR e da FISMA da AWS.
12	Acesso privilegiado. O provedor em nuvem aborda a ameaça de acesso privilegiado inadequado aos dados e aos aplicativos do cliente?	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.
13	Locação múltipla. A diferenciação de cliente é implementada com segurança?	O ambiente da AWS é virtualizado e de locação múltipla. 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 2.0, publicado em outubro de 2010. Observe que 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 o hardware dedicado a um único cliente. Instâncias dedicadas permitem aproveitar ao máximo os benefícios da Amazon VPC e a nuvem da AWS, isolando ao mesmo tempo suas instâncias de computação do Amazon EC2 no nível do hardware.

14	Vulnerabilidades do hipervisor. O provedor em nuvem abordou as vulnerabilidades conhecidas do hypervisor?	O Amazon EC2 atualmente utiliza uma versão altamente personalizada do hipervisor Xen. O hipervisor é regularmente avaliado quanto a 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 hipervisor AWS Xen é regularmente avaliado por auditores independentes durante avaliações e auditorias. Consulte a documentação de segurança da AWS para obter mais informações sobre o isolamento de instância e o hipervisor Xen.
15	Gerenciamento de vulnerabilidades. Os sistemas são corrigidos adequadamente?	A AWS é responsável pela correção dos sistemas que fornecem suporte à disponibilização dos serviços ao cliente, tais como o hipervisor 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 convidados, software e aplicativos; portanto, são responsáveis pela aplicação de correções em seus próprios sistemas.
16	Criptografia. Os serviços prestados oferecem suporte para 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. As sessões da VPC também são criptografadas. O Amazon S3 também oferece criptografia por parte do 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.
17	Propriedade de dados. Quais são os direitos do provedor em nuvem sobre os dados de 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 desafiar ordens legais, se acreditarmos que as mesmas sejam infundadas ou não possuam embasamento sólido.
18	Isolamento de dados. O provedor em nuvem isola adequadamente os dados de cliente?	Todos os dados armazenados pela AWS em nome dos clientes têm ótimos recursos de controle e segurança de isolamento de locação. 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.
19	Serviços compostos. A camada de provedor em nuvem de seu serviço funciona com outros serviços de provedor em nuvem?	A AWS não utiliza provedor de nuvem de terceiros para fornecer serviços da AWS para os clientes.
20	Controles físico e ambiental. Estes controles são operados por um provedor em nuvem especificado?	Sim. Estes são descritos especificamente no relatório SOC 1, tipo II. Além disso, outras certificações utilizadas pela AWS, tais como ISO 27001 e FISMA, exigem práticas recomendadas de controle físico e ambiental.

21	Proteção do cliente. O provedor em nuvem permite a proteção e o gerenciamento do acesso de clientes, tais como PC e dispositivos móveis?	Sim. A AWS permite aos clientes gerenciar os aplicativos móveis e clientes para suas próprias necessidades.
22	Segurança do servidor. O provedor em nuvem permite que os 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 mais detalhes sobre segurança de rede e de servidor.
23	Identity and Access Management. O serviço inclui recursos de IAM?	A AWS tem um pacote de ofertas de gerenciamento de identidade e acesso, que permite aos clientes gerenciar identidades de usuários, atribuir credenciais de segurança, organizar os usuários em grupos e gerenciar permissões de usuário de maneira centralizada. Consulte o site da AWS para obter mais informações.
24	Paralisações 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.
25	Capacidade de escalabilidade. O provedor permite que os clientes utilizem a escalabilidade além do acordo original?	A nuvem da AWS é distribuída, altamente segura e flexível, dando aos clientes enorme potencial de escalabilidade. Os clientes podem expandir para mais ou para menos, pagando apenas pelo que utilizarem.
26	Disponibilidade de serviço. O provedor compromete-se com um alto nível de disponibilidade?	A AWS compromete-se com altos níveis de disponibilidade em seus Acordos de Nível 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 compromete-se com a porcentagem mensal de atividade pelo menos 99,99%. Caso essas métricas de disponibilidade não sejam atendidas, serão fornecidos créditos de serviço. Em 21 de abril de 2011, o EC2 sofreu uma interrupção do serviço ao cliente afetando a região leste dos EUA. Detalhes sobre a interrupção do serviço são descritos no "Summary of the Amazon EC2 and Amazon RDS Service Disruption in the US East Region" (http://aws.amazon.com/message/65648/).
27	Ataques de negação de serviço distribuída (DDoS). Como o provedor protege seu serviço contra ataques de 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 de DDoS.
28	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 S3 acelera a movimentação de grandes volumes de dados internamente e externamente na AWS usando dispositivos de armazenamento portáteis para transporte.

29	Continuidade de negócios do provedor de serviço. O provedor de serviço executa um programa de continuidade de negócios?	A AWS executa um programa de continuidade de negócios. Informações detalhadas são fornecidas no whitepaper de segurança da AWS.
30	Continuidade de negócios do cliente. O provedor de serviço permite que os clientes implementem um plano de continuidade de negócios?	A AWS oferece aos clientes a capacidade de implementar um plano de continuidade robusta, incluindo a utilização de backups frequentes de instância de servidor, replicação de redundância de dados e arquiteturas de implementação da zona de disponibilidade/várias regiões.
31	Durabilidade dos dados. O serviço especifica a durabilidade dos dados?	O Amazon S3 oferece aos clientes uma infraestrutura de armazenamento altamente durável. Os objetos são armazenados redundantemente 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.
32	Backups. O serviço fornece backups em fita?	A AWS permite que os clientes façam seus backups em fitas usando seu próprio provedor de serviço de backup em 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, bem como a durabilidade equivalente de cópias de vários locais de objetos de dados é obtida através de redundância de armazenamento de dados. Para obter informações sobre redundância e durabilidade de dados, consulte o site da AWS.
33	Aumentos de preço. O provedor de serviço aumentará os preços inesperadamente?	A AWS tem uma história de redução frequente de preços, pois o custo para fornecer esses serviços reduz ao longodo tempo. A AWS teve seu preço reduzido de forma consistente durante os últimos anos.
34	Sustentabilidade. A empresa do provedor de serviço tem o potencial de sustentabilidade de longo prazo?	A AWS é um provedor líder de nuvem e é uma estratégia de negócios a longo prazo do Amazon.com. A AWS tem um potencial muito elevado de sustentabilidade a longo prazo.

Contato da AWS

Os clientes podem entrar em contato com a equipe de Conformidade ou Segurança da AWS através de seu representante de desenvolvimento de negócios. O representante encaminha os clientes para a equipe adequada dependendo da natureza da consulta. Como alternativa, perguntas gerais podem ser enviadas para: aws-security@amazon.com

APÊNDICE A – CSA CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE V1.1 (QUESTIONÁRIO DE INICIATIVA DE AVALIAÇÕES DE CONSENSO DA CSA, VERSÃO 1.1)

A Cloud Security Alliance (CSA, Aliança de Segurança em Nuvem) é uma organização "sem fins lucrativos", com uma missão de promover o uso de práticas recomendadas para fornecer garantias de segurança na computação em nuvem, bem como fornecer educação sobre os usos de computação em nuvem para ajudar a proteger todas as outras formas de computação." [Referência https://cloudsecurityalliance.org/about/] Uma ampla variedade de associações, corporações e pessoas do setor de segurança participam desta organização para cumprir sua missão.

O CSA Consensus Assessments Initiative Questionnaire fornece um conjunto de perguntas que a CSA prevê que um consumidor de nuvem e/ou auditor de nuvem faria a um provedor de nuvem. Ele fornece uma série de perguntas de segurança, controle e processo, que podem então ser usadas para uma ampla variedade de usos, incluindo avaliação de segurança e seleção de provedor de nuvem. A AWS concluiu esse questionário com as perguntas a seguir.

Domínio	Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Conformidade	Planejamento de auditoria	CO-01.1	Vocês produzem declarações de auditoria usando um formato estruturado e aceito pelo setor (p. ex., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, Programa de garantia/auditoria de gerenciamento da computação em nuvem da ISACA, etc.)?	A AWS obtém determinadas certificações do setor e declarações de terceiros independentes, e fornece determinadas certificações, relatórios e outra documentação relevante para clientes da AWS sob NDA (acordo de confidencialidade).
Conformidade	Auditorias independentes	CO-02.1	Vocês permitem que locatários vejam seus relatórios SAS70, tipo II/SSAE 16 SOC2/ISAE3402 ou relatórios de auditoria de terceiros semelhantes?	A AWS fornece declarações de terceiros, certificações, relatório de controles de empresa de serviços (SOC 1), tipo II e outros relatórios de conformidade relevantes diretamente para nossos clientes sob NDA. A segurança da AWS examina regularmente todos os endereços IP de endpoint, de serviço voltado à Internet, quanto à existência de vulnerabilidades (essas verificações não incluem instâncias de clientes). A segurança da AWS notificará as partes adequadas para solucionar quaisquer vulnerabilidades identificadas. Além disso, avaliações de ameaça de vulnerabilidade externa são realizadas regularmente por empresas de segurança independentes. As conclusões e recomendações resultantes dessas avaliações são categorizadas e entregues à liderança da AWS. Além disso, o ambiente de controle da AWS está sujeito a avaliações regulares internas e externas de riscos. A AWS contrata órgãos externos de certificação e auditores independentes para analisar e testar o ambiente de controle geral da AWS.
Conformidade		CO-02.2	Vocês realizam regularmente testes de penetração em rede de sua infraestrutura de serviço em nuvem, como prescrito pelas orientações e práticas recomendadas do setor?	
Conformidade		CO-02.3	Vocês realizam regularmente testes de penetração em rede de sua infraestrutura de nuvem, como prescrito pelas orientações e práticas recomendadas do setor?	
Conformidade		CO-02.4	Vocês realizam regularmente auditorias internas, como prescrito pelas orientações e práticas recomendadas do setor?	
Conformidade		CO-02.5	Vocês realizam regularmente auditorias externas, como prescrito pelas orientações e práticas recomendadas do setor?	
Conformidade		CO-02.6	Os resultados de testes de penetração em rede estão disponíveis para locatários mediante solicitação?	
Conformidade		CO-02.7	Os resultados de auditorias internas e externas estão disponíveis para locatários mediante solicitação?	

Conformidade	Auditorias de terceiros	CO-03.1	Vocês permitem que locatários realizem avaliações independentes quanto a vulnerabilidades?	Os clientes podem solicitar permissão para conduzir pesquisas de sua infraestrutura em nuvem, somente se essas se limitarem a instâncias do cliente e não violarem a política de uso aceitável da AWS. A prévia aprovação para esses tipos de verificações pode ser iniciada ao se enviar uma solicitação através do formulário AWS Vulnerability/Penetration Testing Request (Solicitação de teste de penetração/vulnerabilidade da AWS). A segurança da AWS contrata regularmente empresas de segurança independentes para realizar avaliações de ameaça e vulnerabilidade externa. O relatório SOC 1, tipo II, da AWS fornece detalhes adicionais sobre atividades específicas de controle executadas pela AWS.
Conformidade		CO-03.2	Vocês têm terceiros externos que realizam verificações de vulnerabilidade e testes periódicos de penetração em seus aplicativos e redes?	
Conformidade	Manutenção de autoridade/ contato	CO-04.1	Vocês mantêm alianças e pontos de contato com autoridades locais de acordo com contratos e regulamentos apropriados?	A AWS mantém contatos com órgãos do setor, organizações de conformidade e avaliação de riscos, autoridades locais e órgãos normativos, como exigido pelo padrão ISO 27001.
Conformidade	Mapeamento normativo do sistema de informações	CO-05.1	Vocês têm a capacidade de segmentar ou criptografar logicamente os dados de clientes, de forma que esses dados possam ser produzidos somente para um único locatário, sem acessar inadvertidamente os dados de outro locatário?	Todos os dados armazenados pela AWS em nome dos clientes têm ótimos recursos de controle e segurança de isolamento de locação. Os clientes retêm o controle e a propriedade de seus dados; portanto, é sua responsabilidade escolher criptografar os dados. A AWS permite que os clientes usem seus próprios mecanismos de criptografia para quase todos os serviços, incluindo S3, EBS, SimpleDB e EC2. As sessões da VPC também são criptografadas. O Amazon S3 também oferece criptografia por parte do servidor como uma opção para os clientes. Consulte o whitepaper de conformidade e avaliação de riscos da AWS para obter detalhes adicionais - consulte em http://aws.amazon.com/pt/security.
		CO-05.2	Vocês têm capacidade para segmentar e recuperar logicamente dados de um cliente específico no caso de uma falha ou perda de dados?	
Conformidade	Propriedade intelectual	CO-06.1	Vocês têm políticas e procedimentos vigentes descrevendo quais controles estão em vigor para proteger a propriedade intelectual do locatário?	As equipes de conformidade e segurança da AWS estabeleceram políticas e estrutura de segurança da informação com base na estrutura de COBIT (Control Objectives for Information and related Technology). A estrutura de segurança da AWS integra as práticas recomendadas do ISO 27002 e o padrão de segurança de dados do PCI. Consulte o whitepaper de conformidade e avaliação de riscos da AWS para obter detalhes adicionais - consulte em http://aws.amazon.com/pt/security.
Conformidade	Propriedade intelectual	CO-07.1	Se for realizada mineração na utilização de serviços de locatários hospedados na nuvem para benefício do provedor de nuvem, os direitos de IP de locatários serão preservados?	A utilização de recursos é monitorada pela AWS, conforme necessário, para gerenciar eficazmente a disponibilidade do serviço. A AWS não coleta a propriedade intelectual do cliente como parte do monitoramento de utilização de recursos.

Conformidade	Propriedade intelectual	CO-08.1	Se for realizada mineração na utilização de serviços de locatários hospedados na nuvem para benefício do provedor de nuvem, vocês oferecem a opção de recusa para os locatários?	Não é realizada mineração da utilização de serviços de clientes hospedados na nuvem.
Gestão de dados	Propriedade/ administração	DG-01.1	Vocês seguem um padrão estruturado de rótulos de dados (p. ex., ISO 15489, Especificação de catálogo XML Oasis, orientação de tipos de dados da CSA)?	Os clientes da AWS retêm o controle e a propriedade de seus dados e podem implementar um padrão estruturado de rótulos de dados para atender às suas exigências.
Gestão de dados	Classificação	DG-02.1	Vocês fornecem recursos para identificar máquinas virtuais via metadados/tags de política (p. ex., tags podem ser usadas para limitar sistemas operacionais convidados de inicializar/instanciar/transportar dados no país errado, etc.)?	As máquinas virtuais são designadas a clientes como parte do serviço EC2. Os clientes retêm o controle sobre quais recursos estão sendo usados e onde eles residem. Consulte o site da AWS para obter detalhes adicionais - http://aws.amazon.com.
Gestão de dados		DG-02.2	Vocês fornecem recursos para identificar hardware via tags/metadados/tags de hadware (p. ex., TXT/TPM, tag VN, etc.)?	A AWS fornece a capacidade para utilizar tags em recursos do EC2. Como uma forma de metadados, as tags do EC2 podem ser usadas para criar nomes acessíveis, aprimorar a capacidade de pesquisa e melhorar a coordenação entre vários usuários. O AWS Management Console também oferece suporte ao uso de tags.
Gestão de dados		DG-02.3	Vocês têm recursos para usar localização geográfica de sistema como um fator de autenticação?	A AWS fornece a capacidade de acesso de usuário condicional com base em endereço IP. Os clientes podem acrescentar condições para controlar como os usuários podem utilizar a AWS, como o horário do dia, seu endereço IP originário e se eles estão usando SSL.
Gestão de dados		DG-02.4	Vocês podem fornecer a localização física/geografia de armazenamento de dados de um locatário mediante solicitação?	A AWS oferece aos clientes a flexibilidade de alocar instâncias e armazenar dados em várias regiões geográficas. Os clientes da AWS determinam a região física em que seus dados e seus servidores estarão localizados. A AWS não moverá o conteúdo de clientes das Regiões selecionadas sem notificar o cliente, exceto se necessário para cumprir a legislação ou solicitações de entidades governamentais. A AWS atualmente oferece oito regiões: Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Norte da Califórnia), Oeste dos EUA (Oregon), GovCloud (EUA) (Oregon), UE (Irlanda), Ásia-Pacífico (Cingapura), Ásia-Pacífico (Tóquio) e América do Sul (São Paulo). Consulte o whitepaper de conformidade e avaliação de riscos da AWS para obter detalhes adicionais - consulte em http://aws.amazon.com/pt/security.
Gestão de dados		DG-02.5	Vocês permitem que locatários definam locais geográficos aceitáveis para roteamento de dados ou instanciação de recursos?	
Gestão de dados	Política de segurança/ rotulamento/ identificação	DG-03.1	Há políticas e procedimentos estabelecidos para rotulamento, identificação e segurança de dados e objetos que contêm dados?	Os clientes da AWS retêm controle e propriedade de seus dados e podem implementar procedimentos e política de identificação e rotulagem, a fim de atender às suas exigências.
Gestão de dados		DG-03.2	Há mecanismos de herança de rótulo implementados para objetos que atuam como recipientes agregados para dados?	

Gestão de dados	Política de retenção	DG-04.1	Vocês têm capacidades de controle técnico para aplicar políticas de retenção de dados de locatário?	A AWS fornece aos clientes a capacidade de excluir seus dados. No entanto, os clientes da AWS retêm controle e propriedade de seus dados; portanto, é de responsabilidade do cliente gerenciar a retenção de dados de acordo com seus próprios requisitos. Consulte o whitepaper de visão geral dos processos de segurança da AWS para obter detalhes adicionais - consulte em http://aws.amazon.com/pt/security. 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 desafiar ordens legais, se acreditarmos que tais são infundadas ou não possuem embasamento sólido.
Gestão de dados		DG-04.2	Vocês têm um procedimento documentado para responder a solicitações de dados de locatários de governos ou terceiros?	
Gestão de dados	Descarte seguro	DG-05.1	Vocês oferecem suporte à exclusão segura (p. ex., limpeza criptográfica/inutilização) de dados arquivados como determinado pelo locatário?	Quando um dispositivo de armazenamento tiver atingido o final da sua vida útil, os procedimentos da AWS incluirão um processo de desativação que é projetado para impedir que os dados do cliente sejam expostos a pessoas não autorizadas. A AWS usa as técnicas detalhadas no DoD 5220.22-M ("Manual operacional do programa de segurança industrial nacional") ou NIST 800-88 ("Orientações para o tratamento de mídia") para destruir dados como parte do processo de desativação. Se um dispositivo de hardware for incapaz de ser desativado usando esses procedimentos, o dispositivo será inutilizado ou fisicamente destruído em conformidade com as práticas padrão do setor. Consulte o whitepaper de visão geral de processos de segurança da AWS para obter detalhes adicionais - consulte em http://aws.amazon.com/pt/security.
Gestão de dados		DG-05.2	Vocês podem fornecer um procedimento publicado para saída da disposição do serviço, incluindo garantia de tratamento de todos os recursos de computação de dados do locatário assim que o cliente tiver saído de seu ambiente ou tiver liberado um recurso?	
Gestão de dados	Dados não relativos à produção	DG-06.1	Vocês têm procedimentos vigentes para garantir que os dados de produção não serão replicados ou usados em ambientes não relativos à produção?	Os clientes da AWS mantêm o controle e a propriedade sobre os seus próprios dados. A AWS fornece aos clientes a capacidade de manter e desenvolver ambientes de produção e não relativos à produção. É de responsabilidade do cliente garantir que seus dados de produção não sejam replicados para ambientes que não sejam de produção.

Gestão de dados	Vazamento de informações	DG-07.1	Vocês têm controles vigentes para impedir o vazamento de dados ou comprometimento intencional/acidental entre locatários em um ambiente de vários locatários?	O ambiente da AWS é virtualizado e de locação múltipla. 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 QSA (Qualified Security Assessor, Assessor qualificado em segurança) do PCI independente e foi determinada como estando em conformidade com todos os requisitos do PCI DSS versão 2.0 publicado em junho de 2011. Consulte o whitepaper de conformidade e avaliação de riscos da AWS para obter detalhes adicionais - consulte em http://aws.amazon.com/pt/security.
Gestão de dados		DG-07.2	Vocês têm uma solução de prevenção de extrusões ou DLP (Data Loss Prevention, Prevenção de perda de dados) vigente para todos os sistemas que interagem com sua oferta de serviço em nuvem?	
Gestão de dados	Avaliações de riscos	DG-08.1	Vocês fornecem dados de saúde de controle de segurança, a fim de permitir que locatários implementem monitoramento contínuo padrão do setor (que permite a validação contínua de locatário de seu status de controle físico e lógico)?	A AWS publica relatórios de auditores independentes e certificações para fornecer aos clientes informações consideráveis em relação às políticas, aos processos e aos controles estabelecidos e operados pela AWS. Os relatórios e certificações relevantes podem ser fornecidos a clientes da AWS. O monitoramento contínuo de controles lógicos pode ser executado por clientes em seus próprios sistemas.
Segurança de instalações	Política	FS-01.1	Vocês podem fornecer evidências de que foram estabelecidos procedimentos e políticas para manter um ambiente de trabalho seguro e protegido em escritórios, salas, instalações e áreas seguras?	A AWS contrata órgãos externos de certificação e auditores independentes para analisar e validar nossa conformidade com estruturas de conformidade. O relatório SOC 1, tipo II, da AWS fornece detalhes adicionais sobre atividades específicas de controle de segurança física executadas pela AWS. Consulte o padrão ISO 27001, Anexo A, domínio 9.1 para obter mais detalhes. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Segurança de instalações	Acesso de usuário	FS-02.1	De acordo com as restrições contratuais, ética, regulamentos e legislações locais, todos os candidatos à contratação, contratantes e terceiros estão sujeitos à verificação de antecedentes?	A AWS realiza verificações de antecedentes criminais, como permitido pela legislação aplicável, como parte das práticas de triagem antes da contratação de funcionários, de acordo com a posição e nível de acesso do funcionário a instalações da AWS.

Segurança de instalações	Pontos de acesso controlado	FS-03.1	Há perímetros de segurança física (cercas, muros, barreiras, vigias, portões, vigilância eletrônica, mecanismos de autenticação física, locais de recepção e portas de segurança) implementados?	Os controles de segurança física incluem, mas não estão limitados a, controles de perímetro como cerca, muros, equipe de segurança, vigilância com vídeo, sistemas de detecção de intrusão e outros meios eletrônicos. O relatório SOC 1, tipo II, da AWS fornece detalhes adicionais sobre atividades específicas de controle executadas pela AWS. Consulte o padrão ISO 27001, Anexo A, domínio 9.1 para obter mais informações. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Segurança de instalações	Autorização de área segura	FS-04.1	Vocês permitem que locatários especifiquem em quais de seus locais geográficos seus dados têm permissão para entrar/sair (para atender a considerações jurisdicionais legais com base em onde os dados são armazenados versus acessados)?	Os clientes da AWS podem designar em qual região física seus dados e seus servidores estarão localizados. A AWS não moverá o conteúdo de clientes das Regiões selecionadas sem notificar o cliente, exceto se necessário para cumprir a legislação ou solicitações de entidades governamentais. A AWS atualmente oferece oito regiões: Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Norte da Califórnia), Oeste dos EUA (Oregon), GovCloud (EUA) (Oregon), UE (Irlanda), Ásia-Pacífico (Cingapura), Ásia-Pacífico (Tóquio) e América do Sul (São Paulo). Consulte o site da AWS em http://aws.amazon.com para obter detalhes adicionais.
Segurança de instalações	Entrada de pessoas não autorizadas	FS-05.1	Há pontos de entrada e saída, como áreas de serviço e outros pontos em que pessoal não autorizado pode entrar em locais monitorados, controlados e isolados de processo e armazenamento de dados?	O acesso físico é estritamente controlado no perímetro e nos pontos de ingresso de prédios pelos funcionários de segurança profissional utilizando a vigilância por vídeo, sistemas de detecção de intrusão e outros meios eletrônicos. O pessoal autorizado deve passar pela autenticação de dois fatores, no mínimo duas vezes, para ter acesso aos andares do datacenter. Consulte o whitepaper de visão geral de processos de segurança da AWS para obter detalhes adicionais, disponível em http://aws.amazon.com/pt/security. Além disso, o relatório SOC 1, tipo II, da AWS fornece detalhes adicionais sobre atividades específicas de controle executadas pela AWS.
Segurança de instalações	Autorização fora do local	FS-06.1	Vocês fornecem aos locatários documentação que descreva cenários em que os dados podem ser movidos de um local físico para outro (por exemplo, replicação, failovers de continuidade de negócios, backups fora do local)?	Os clientes da AWS podem designar em qual região física seus dados estarão localizados. A AWS não moverá o conteúdo de clientes das Regiões selecionadas sem notificar o cliente, exceto se necessário para cumprir a legislação ou solicitações de entidades governamentais. Consulte o whitepaper de visão geral de processos de segurança da AWS para obter detalhes adicionais - consulte em http://aws.amazon.com/pt/security.

Segurança de instalações	Equipamento fora do local	FS-07.1	Vocês fornecem aos locatários documentação descrevendo suas políticas e procedimentos regendo gerenciamento de ativos e realocação de equipamento?	Em alinhamento com os padrões do ISO 27001, quando um dispositivo de armazenamento atingiu o final da sua vida útil, os procedimentos da AWS incluem um processo de desativação que é projetado para impedir que os dados do cliente sejam expostos a pessoas não autorizadas. A AWS usa as técnicas detalhadas no DoD 5220.22-M ("Manual operacional do programa de segurança industrial nacional") ou NIST 800-88 ("Orientações para o tratamento de mídia") para destruir dados como parte do processo de desativação. Se um dispositivo de hardware é incapaz de ser desativado usando esses procedimentos, o dispositivo será inutilizado ou fisicamente destruído em conformidade com as práticas padrão do setor. Consulte o padrão ISO 27001, Anexo A, dominio 9.2 para obter mais detalhes. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Segurança de instalações	Gerenciamento de ativos	FS-08.1	Vocês mantêm um inventário completo de todos os seus ativos críticos, que inclui propriedade do ativo?	Em alinhamento com os padrões do ISO 27001, os ativos de hardware da AWS são atribuídos a um proprietário, controlados e monitorados pela equipe da AWS, com ferramentas de gerenciamento de inventário de propriedade da AWS. A equipe da cadeia de fornecimento e aquisição da AWS mantém relações com todos os fornecedores da AWS. Consulte o padrão ISO 27001, Anexo A, dominio 7.1 para obter mais detalhes. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Segurança de instalações		FS-08.2	Vocês mantêm um inventário completo de todas as suas relações com fornecedores essenciais?	
Segurança de recursos humanos	Triagem de histórico	HR-01.1	De acordo com as restrições contratuais, ética, regulamentos e legislações locais, todos os candidatos à contratação, contratantes e terceiros estão sujeitos à verificação de antecedentes?	A AWS realiza verificações de antecedentes criminais, como permitido pela legislação aplicável, como parte das práticas de triagem antes da contratação de funcionários, de acordo com a posição e nível de acesso do funcionário a instalações da AWS. Consulte o whitepaper de visão geral de processos de segurança da AWS para obter detalhes adicionais - consulte em http://aws.amazon.com/pt/security.
Segurança de recursos humanos	Contratos empregatícios	HR-02.1	Vocês treinam especificamente seus funcionários em relação à sua função versus a função do locatário em fornecer controles de segurança da informação?	Cada funcionário recebe o Código de ética e conduta nos negócios da empresa e conclui treinamento periódico sobre segurança da informação, que requer uma confirmação de conclusão. As auditorias de conformidade são realizadas periodicamente para validar que os funcionários entendem e seguem as políticas estabelecidas. Consulte o whitepaper de visão geral de processos de segurança da AWS para obter detalhes adicionais - consulte em http://aws.amazon.com/pt/security.
		HR-02.2	Vocês documentam a confirmação do treinamento que o funcionário concluiu?	

Segurança de recursos humanos	Término de contratação	HR-03.1	As funções e responsabilidades para acompanhar a realização de término de contrato ou alteração em procedimentos de contratação são atribuídas, documentadas e comunicadas?	A equipe de recursos humanos da AWS define responsabilidades de gerenciamento interno a serem seguidas para término e alteração de função de funcionários e fornecedores. A responsabilidade pelo provisionamento/ desprovisionamento do acesso do contratante e do funcionário é compartilhada entre proprietários de serviço, operações corporativas e recursos humanos (RH). Consulte o whitepaper de visão geral de processos de segurança da AWS para obter detalhes adicionais - consulte em http://aws.amazon.com/pt/security.
Segurança da informação	Programa de gerenciamento	IS-01.1	Vocês fornecem aos locatários documentação descrevendo seu ISMP (Information Security Management Program, Programa de gerenciamento de segurança da informação)?	A AWS fornece a nossos clientes nossa documentação de certificação ISO 27001, que comunica o programa ISMS da AWS.
Segurança da informação	Envolvimento/ suporte de gerenciamento	IS-02.1	Há políticas vigentes para garantir que executivos e o gerenciamento de linha tomem ações formais para oferecer suporte à segurança da informação através de orientações claras documentadas, comprometimento, atribuição explícita e verificação de execução de atribuição?	Em alinhamento com os padrões do ISO 27001, foram estabelecidos procedimentos e políticas através da estrutura de segurança da informação da AWS. O ambiente de controle na Amazon inicia no mais alto nível da empresa. As liderança executiva e sênior desempenham um papel importante no estabelecimento de valores fundamentais e objetivo da empresa. Consulte o whitepaper de conformidade e avaliação de riscos da AWS para obter detalhes adicionais - consulte em http://aws.amazon.com/pt/security.
Segurança da informação	Política	IS-03.1	Suas políticas de privacidade e segurança da informação estão alinhadas a padrões específicos do setor (ISO-27001, ISO-22307, CoBIT, etc.)?	Foram estabelecidos procedimentos e políticas pela segurança da informação da AWS, com base na estrutura de COBIT, padrões do ISO 27001 e requisitos de PCI DSS. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001. Além disso, a AWS publica um relatório SOC 1, tipo II. Consulte o relatório SOC 1 para obter mais detalhes. Consulte o whitepaper de conformidade e avaliação de riscos da AWS para obter detalhes adicionais, disponível em http://aws.amazon.com/pt/security.
		IS-03.2	Vocês têm contratos que garantem que seus provedores seguem suas políticas de privacidade e segurança da informação?	
		IS-03.3	Vocês podem fornecer evidências de mapeamento de auditoria detalhada de seus controles, arquitetura e processos para regulamentos e/ou padrões?	
Segurança da informação	Requisitos da linha de base	IS-04.1	Vocês têm linhas de base de segurança da informação documentadas para cada componente de sua infraestrutura (p. ex., hipervisores, sistemas operacionais, roteadores, servidores DNS, etc.)?	Em alinhamento com os padrões ISO 27001, a AWS mantém linhas de base de sistema para componentes essenciais. Consulte o padrão ISO 27001, Anexo A, domínios 12.1 e 15.2 para obter mais detalhes. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Segurança da informação		IS-04.2	Vocês têm um recurso para monitorar continuamente e reportar a conformidade de sua infraestrutura em relação às suas linhas de base de segurança da informação?	

Segurança da informação		IS-04.3	Vocês permitem que clientes forneçam sua própria imagem de máquina virtual confiável, a fim de garantir a conformidade com seus próprios padrões internos?	Os clientes podem fornecer sua própria imagem de máquina virtual. O VM Import permite que os clientes importem facilmente imagens de máquina virtual do ambiente existente para instâncias do Amazon EC2.
Segurança da informação	Revisões de política	IS-05.1	Vocês notificam seus locatários quando fazem alterações materiais em suas políticas de privacidade e/ou segurança da informação?	Os whitepapers sobre conformidade e avaliações de risco e visão geral de processos de segurança da AWS, disponíveis em http://aws.amazon.com/pt/security são atualizados regularmente para refletir as modificações em políticas da AWS.
Segurança da informação	Aplicação de política	IS-06.1	Há uma política de sanção ou disciplinar formal estabelecida para funcionários que violaram procedimentos e políticas de segurança?	A AWS fornece política de segurança e oferece treinamento em segurança para funcionários, a fim de instrui-los em sua função e responsabilidades relativas à segurança da informação. Os funcionários que violarem protocolos ou padrões da Amazon serão investigados e serão submetidos à ação disciplinar apropriada (p. ex., advertência, plano de desempenho, suspensão e/ou rescisão). Consulte o whitepaper de visão geral de processos de segurança da AWS para obter detalhes adicionais - disponíveis em http://aws.amazon.com/pt/security. Consulte o padrão ISO 27001, Anexo A, domínio 8.2 para obter mais detalhes. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Segurança da informação		IS-06.2	Os funcionários estão cientes de qual ação poderá ser tomada na hipótese de uma violação? Isso é declarado nas políticas e procedimentos?	
Segurança da informação	Política de acesso de usuário	IS-07.1	Vocês têm controles vigentes para garantir a remoção em tempo hábil de acessos ao sistema que não sejam mais necessários para fins comerciais?	O acesso é revogado automaticamente quando o registro de um funcionário é finalizado no sistema de recursos humanos da Amazon. Quando ocorrem alterações em função do trabalho do funcionário, a continuidade de acesso deve ser explicitamente aprovada para o recurso ou será automaticamente revogada. O relatório SOC 1, tipo II, da AWS fornece mais detalhes sobre a revogação de acesso de usuário. Além do whitepaper de segurança da AWS, a seção "Ciclo de vida do funcionário" fornece informações adicionais. Consulte o padrão ISO 27001, Anexo A, dominio 11 para obter mais detalhes. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Segurança da informação		IS-07.2	Vocês fornecem métricas que controlam com que rapidez é possível remover o acesso a sistemas que não seja mais necessário para fins comerciais?	
Segurança da informação	Autorização/ restrição de acesso de usuário	IS-08.1	Vocês documentam como concedem e aprovam o acesso a dados de locatário?	Os clientes da AWS mantêm o controle e a propriedade sobre os seus dados. Os clientes são responsáveis pelo desenvolvimento, conteúdo, operação, manutenção e uso de seu conteúdo.
Segurança da informação		IS-08.2	Vocês têm um método de alinhamento das metodologias de classificação de dados de locatário e provedor para fins de controle de acesso?	

Segurança da informação	Revogação de acesso de usuário	IS-09.1	O desprovisionamento, revogação ou modificação em tempo hábil de acesso de usuários aos sistemas de organizações, ativos de informações e dados são implementados mediante qualquer alteração no status de funcionários, contratantes, clientes, parceiros comerciais ou terceiros?	O acesso é revogado automaticamente quando o registro de um funcionário é finalizado no sistema de recursos humanos da Amazon. Quando ocorrem alterações em função do trabalho do funcionário, a continuidade de acesso deve ser explicitamente aprovada para o recurso ou será automaticamente revogada. O relatório SOC 1, tipo II, da AWS fornece mais detalhes sobre a revogação de acesso de usuário. Além do whitepaper de segurança da AWS, a seção "Ciclo de vida do funcionário" fornece informações adicionais. Consulte o padrão ISO 27001, Anexo A, dominio 11 para obter mais detalhes. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Segurança da informação		IS-09.2	Alterações no status incluem término de contratação, contrato ou acordo, alteração de contratação ou transferência na organização?	
Segurança da informação	Revisões de acesso de usuário	IS-10.1	Vocês exigem, pelo menos, uma certificação anual de qualificações de todos os administradores e usuários do sistema (exceto usuários mantidos por seus locatários)?	Em alinhamento com o padrão ISO 27001, todas as concessões de acesso são revisadas a cada 90 dias; a reaprovação explícita é necessária ou o acesso ao recurso será automaticamente revogado. Os controles específicos para revisões de acesso de usuário são descritos no relatório SOC 1, tipo II. As exceções nos controles de qualificação de usuário são documentadas no relatório SOC 1, tipo II. Consulte o padrão ISO 27001, Anexo A, dominio 11.2 para obter mais detalhes. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Segurança da informação		IS-10.2	Se for detectado que os usuários não têm as qualificações necessárias, todas as ações de atualização e certificação serão registradas?	
Segurança da informação		IS-10.3	Vocês compartilham relatórios de atualização e certificação de qualificação de usuários com seus locatários no caso de acesso não adequado ter sido permitido a dados de locatários?	
Segurança da informação	Treinamento/ Familiarização	IS-11.1	Vocês fornecem ou disponibilizam um programa de treinamento formal de familiarização em segurança para questões de gerenciamento de dados e acesso relacionado à nuvem (ou seja, vários locatários, nacionalidade, diferenciação de implicações de direitos no modelo de fornecimento em nuvem e conflitos de interesses) para todas as pessoas que acessam os dados de locatários?	Em alinhamento com o padrão ISO 27001, todos os funcionários da AWS realizam treinamento periódico em segurança da informação, o qual requer que uma confirmação para sua conclusão. As auditorias de conformidade são realizadas periodicamente para validar que os funcionários entendem e seguem as políticas estabelecidas.
Segurança da informação		IS-11.2	Os administradores de dados e gerentes são devidamente instruídos sobre suas responsabilidades legais em relação à segurança e à integridade de dados?	
Segurança da informação	Comparação/ conhecimento do setor	IS-12.1	Vocês participam de associações profissionais e grupos do setor relacionados à segurança da informação?	As equipes de segurança e conformidade da AWS mantêm contatos com grupos do setor e serviços profissionais relacionados à segurança. A AWS estabeleceu políticas e uma estrutura de segurança da informação com base na estrutura COBIT e integrou a estrutura certificável por ISO 27001 com base em controles ISO 27002 e PCI DSS. Consulte o whitepaper de conformidade e avaliação de riscos da AWS para obter mais detalhes - disponível em http://aws.amazon.com/pt/security.
		IS-12.2	Vocês comparam seus controles de segurança em relação aos padrões do setor?	

Segurança da informação	Funções/ responsabilidades	IS-13.1	Vocês fornecem aos locatários um documento de definição de função esclarecendo suas responsabilidades administrativas versus as do locatário?	Os whitepapers de visão geral de processos de segurança e de conformidade e avaliação de riscos da AWS fornecem detalhes sobre as funções e responsabilidades da AWS e as de nossos clientes. A área de whitepapers está disponível em: http://aws.amazon.com/pt/security.
Segurança da informação	Supervisão de gerenciamento	IS-14.1	Os gerentes são responsáveis por manter a familiarização e o cumprimento de padrões, procedimentos e políticas de segurança que sejam relevantes para sua área de responsabilidade?	O ambiente de controle na Amazon inicia no mais alto nível da empresa. As liderança executiva e sênior desempenham um papel importante no estabelecimento de valores fundamentais e objetivo da empresa. Cada funcionário recebe o código de conduta e ética nos negócios da empresa, bem como realiza treinamentos periódicos. As auditorias de conformidade são realizadas para que os funcionários entendam e sigam as políticas estabelecidas. Consulte o whitepaper de conformidade e avaliação de riscos da AWS para obter detalhes adicionais - consulte em http://aws.amazon.com/pt/security.
Segurança da informação	Diferenciação de direitos	IS-15.1	Vocês fornecem aos locatários documentação sobre como manter a diferenciação de direitos em sua oferta de serviço em nuvem?	Os clientes detêm a capacidade de gerenciar diferenciações de direitos de seus recursos da AWS. Internamente, a AWS alinha-se com o padrão ISO 27001 para gerenciamento de diferenciação de direitos. Consulte o padrão ISO 27001, Anexo A, domínio 10.1 para obter mais detalhes. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Segurança da informação	Responsabilidade do usuário	IS-16.1	Os usuários estão cientes de suas responsabilidades por manter a familiarização e conformidade com requisitos normativos aplicáveis, padrões, procedimentos e políticas de segurança publicadas?	A AWS implementou diversos métodos de comunicação interna em nível mundial, a fim de ajudar os funcionários a compreenderem suas responsabilidades e funções individuais e a comunicarem eventos significativos em tempo hábil. Esses métodos incluem programas de treinamento e orientação para funcionários recém-contratados, bem como mensagens de e-mail e a publicação de informações via intranet da Amazon. Consulte o padrão ISO 27001, Anexo A, domínios 8.2 e 11.3. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001. Além disso, o whitepaper de visão geral de processos de segurança da AWS para obter detalhes adicionais - disponíveis em http://aws.amazon.com/pt/security.
Segurança da informação		IS-16.2	Os usuários estão cientes de suas responsabilidades por manter um ambiente de trabalho seguro e protegido?	
Segurança da informação		IS-16.3	Os usuários estão cientes de suas responsabilidades por deixar equipamentos não assistidos de forma segura?	
Segurança da informação	Área de trabalho	IS-17.1	Seus procedimentos e políticas de gerenciamento de dados atendem aos conflitos de interesses em nível de serviço e locatário?	As políticas de gerenciamento de dados da AWS estão alinhadas com o padrão ISO 27001. Consulte o padrão ISO 27001, Anexo A, domínios 8.2 e 11.3. A AWS foi validada e

Segurança da informação		IS-17.2	Seus procedimentos e políticas de gerenciamento de dados incluem uma auditoria de adulteração ou função de integridade de software por acesso não autorizado aos dados do locatário?	certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001. O relatório SOC 1, tipo 2, da AWS fornece detalhes adicionais sobre atividades específicas de controle executadas pela AWS para impedir o acesso não autorizado a recursos da AWS.
Segurança da informação		IS-17.3	A infraestrutura de gerenciamento de máquina virtual inclui uma auditoria de adulteração ou função de integridade de software, a fim de detectar alterações na compilação/configuração da máquina virtual?	
Segurança da informação	Criptografia	IS-18.1	Vocês têm recursos para permitir a criação de chaves de criptografia exclusivas por locatário?	Os clientes da AWS gerenciam sua própria criptografia, exceto que estão utilizando o serviço de criptografia do servidor da AWS. Nesse caso, a AWS não cria uma chave de criptografia exclusiva por locatário. Consulte o whitepaper de visão geral de processos de segurança da AWS para obter detalhes adicionais - consulte em http://aws.amazon.com/pt/security.
Segurança da informação		IS-18.2	Vocês oferecem suporte a chaves de criptografia geradas por locatário ou permitem que locatários criptografem dados em uma identidade, sem acesso a um certificado de chave pública (por exemplo, criptografia baseada em identidade)?	
Segurança da informação	Gerenciamento de chave de criptografia	IS-19.1	Vocês criptografam dados de locatário em repouso (em disco/armazenamento) em seu ambiente?	A AWS permite que os clientes usem seus próprios mecanismos de criptografia para quase todos os serviços, incluindo S3, EBS, SimpleDB e EC2. As sessões da VPC também são criptografadas. O Amazon S3 também oferece criptografia por parte do servidor como uma opção para os clientes. Os clientes também podem usar tecnologias de criptografia de terceiros. Os procedimentos de gerenciamento de chaves da AWS estão alinhados com o padrão ISO 27001. Consulte o padrão ISO 27001, Anexo A, domínio 15.1 para obter mais detalhes. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001. Consulte o whitepaper de visão geral de processos de segurança da AWS para obter detalhes adicionais - consulte em http://aws.amazon.com/pt/security.
Segurança da informação		IS-19.2	Vocês utilizam criptografia para proteger imagens de máquina virtual e dados durante o transporte em e entre instâncias de hipervisor e redes?	
Segurança da informação		IS-19.3	Vocês têm recursos para gerenciar chaves de criptografia em nome de locatários?	
Segurança da informação		IS-19.4	Vocês mantêm procedimentos de gerenciamento de chaves?	
Segurança da informação	Gerenciamento de aplicação de correções/ vulnerabilidades	IS-20.1	Vocês realizam regularmente verificações de vulnerabilidade na camada de rede, como prescrito por práticas recomendadas do setor?	Os clientes detêm o controle de seus próprios sistemas operacionais convidados, software e aplicativos. Além disso, são responsáveis por realizar verificações de vulnerabilidade e aplicação de correções em seus próprios sistemas. Os clientes podem solicitar permissão para conduzir pesquisas de sua infraestrutura em nuvem, somente se essas se limitarem a instâncias do cliente e não violarem a política de uso aceitável da AWS. A segurança da AWS examina regularmente todos os endereços IP de endpoint, de serviço voltado à Internet, quanto à existência de vulnerabilidades. A segurança da
Segurança da informação		IS-20.2	Vocês realizam verificações de vulnerabilidade na camada de aplicativos regularmente, como prescrito por práticas recomendadas do setor?	
Segurança da informação		IS-20.3	Vocês realizam verificações de vulnerabilidade na camada de sistemas operacionais locais regularmente, como prescrito por práticas recomendadas do setor?	

Segurança da informação		IS-20.4	Os resultados de verificações de vulnerabilidade estarão disponíveis para locatários mediante solicitação?	AWS notificará as partes adequadas para solucionar quaisquer vulnerabilidades identificadas. A manutenção da AWS e a aplicação de correções de sistema geralmente não afetam os clientes. Consulte o whitepaper de visão geral de processos de segurança da AWS para obter detalhes adicionais, disponível em http://aws.amazon.com/pt/security. Consulte o padrão ISO 27001, Anexo A, dominio 12.5 para obter mais detalhes. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Segurança da informação		IS-20.5	Vocês têm um recurso para aplicar rapidamente correções em todos os seus sistemas, aplicativos e dispositivos de computação?	
Segurança da informação		IS-20.6	Vocês fornecerão intervalos de tempo para a aplicação de correções em sistemas, com base em riscos, para seus locatários mediante solicitação?	
Segurança da informação	Software mal-intencionado/ antivírus	IS-21.1	Vocês têm programas antimalware instalados em todos os sistemas compatíveis com ofertas de serviço em nuvem?	Os procedimentos, processos e programa da AWS para gerenciar software mal-intencionado/antivírus estão em alinhamento com os padrões ISO 27001. Para obter mais detalhes, consulte o relatório SOC 1, tipo II. Além disso, consulte o padrão ISO 27001, Anexo A, domínio 10.4 para obter mais detalhes. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Segurança da informação		IS-21.2	Você garante que sistemas de detecção de ameaças de segurança que usam assinaturas, listas ou padrões comportamentais são atualizados em todos os componentes de infraestrutura dentro dos intervalos de tempo aceitáveis do setor?	
Segurança da informação	Gerenciamento de incidentes	IS-22.1	Vocês têm um plano documentado de resposta a incidentes de segurança?	Os procedimentos, planos e programa de resposta a incidentes da AWS foram desenvolvidos em alinhamento com o padrão ISO 27001. O relatório SOC 1, tipo II, da AWS fornece detalhes sobre atividades específicas de controle executadas pela AWS. O whitepaper de visão geral de processos de segurança da AWS (disponível em http://aws.amazon.com/pt/security) fornece detalhes adicionais.
Segurança da informação		IS-22.2	Vocês integram exigências personalizadas de locatário aos seus planos de resposta a incidentes de segurança?	
Segurança da informação		IS-22.3	Vocês publicam um documento com funções e responsabilidades especificando pelo que vocês versus seus locatários são responsáveis durante incidentes de segurança?	
Segurança da informação	Relatório de incidentes	IS-23.1	Seu sistema de SIEM (Security information and Event Management, Gerenciamento de eventos e informações de segurança) mescla origens de dados (logs de aplicativos, logs de firewall, logs de IDs, logs de acesso físico, etc.) para alertas e análise granular?	Os procedimentos, planos e programa de resposta a incidentes da AWS foram desenvolvidos em alinhamento com o padrão ISO 27001. O relatório SOC 1, tipo II, da AWS fornece detalhes sobre atividades específicas de controle executadas pela AWS. Todos os dados armazenados pela AWS em nome dos clientes têm ótimos recursos de controle e segurança de isolamento de locação. Consulte os whitepapers de visão geral de processos de segurança e de conformidade e avaliação de riscos da AWS (disponíveis em http://aws.amazon.com/pt/security) para obter detalhes adicionais.
Segurança da informação		IS-23.2	A sua estrutura de monitoramento e registro de logs permite o isolamento de um incidente para locatários específicos?	

Segurança da informação	Preparação legal de resposta a incidentes	IS-24.1	O seu plano de resposta a incidentes está em conformidade com os padrões do setor para controles e processos de gerenciamento de cadeia de custódia legalmente admissíveis?	Os procedimentos, planos e programa de resposta a incidentes da AWS foram desenvolvidos em alinhamento com o padrão ISO 27001. O relatório SOC 1, tipo II, da AWS fornece detalhes sobre atividades específicas de controle executadas pela AWS. Todos os dados armazenados pela AWS em nome dos clientes têm ótimos recursos de controle e segurança de isolamento de locação. Consulte os whitepapers de visão geral de processos de segurança e de conformidade e avaliação de riscos da AWS (disponíveis em http://aws.amazon.com/pt/security) para obter detalhes adicionais.
Segurança da informação		IS-24.2	O seu recurso de resposta a incidentes inclui o uso de técnicas forenses de análise e coleta de dados legalmente admissíveis?	
Segurança da informação		IS-24.3	Vocês são capazes de suportar suspensões por litígio ("congelamento" de dados de um ponto específico de tempo) para um locatário específico sem "congelar" dados de outros locatários?	
Segurança da informação		IS-24.4	Vocês aplicam e atestam separação de dados de locatários ao produzir dados em resposta a citações judiciais?	
Segurança da informação	Métricas de resposta a incidentes	IS-25.1	Vocês monitoram e quantificam os tipos, volumes e impactos em todos os incidentes de segurança da informação?	As métricas de segurança da AWS são monitoradas e analisadas de acordo com o padrão ISO 27001. Consulte o padrão ISO 27001, Anexo A, dominio 13.2 para obter mais detalhes. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Segurança da informação		IS-25.2	Vocês compartilharão dados de incidentes de segurança de informações estatísticas com seus locatários mediante solicitação?	
Segurança da informação	Uso aceitável	IS-26.1	Vocês fornecem documentação em relação a como podem utilizar ou acessar metadados e/ou dados de locatários?	Os clientes da AWS mantêm o controle e a propriedade sobre os seus dados.
Segurança da informação		IS-26.2	Vocês coletam ou criam metadados sobre uso de dados de locatário através do uso de tecnologias de inspeção (mecanismos de pesquisa, etc.)?	
Segurança da informação		IS-26.3	Vocês permitem que locatários neguem o acesso a seus dados/metadados através de tecnologias de inspeção?	
Segurança da informação	Devoluções de ativos	IS-27.1	Há sistemas vigentes para monitorar violações de privacidade e notificar os locatários imediatamente se um evento de privacidade puder ter afetado seus dados?	Os clientes da AWS têm a responsabilidade por monitorar seu próprio ambiente quanto a violações de privacidade. O relatório SOC 1, tipo II, da AWS fornece uma visão geral dos controles vigentes para monitorar o ambiente gerenciado da AWS.
Segurança da informação		IS-27.2	Sua política de privacidade está alinhada com os padrões do setor?	
Segurança da informação	Transações de comércio eletrônico	IS-28.1	Vocês fornecem metodologias de criptografia aberta (3.4ES, AES, etc.) para locatários, a fim de solicitar que eles protejam seus dados se for necessário atravessar redes públicas (por exemplo, a Internet)?	Todas as APIs da AWS estão disponíveis através de endpoints protegidos por SSL que fornecem autenticação de servidor. A AWS permite que os clientes usem seus próprios mecanismos de criptografia para quase todos os serviços, incluindo S3, EBS, SimpleDB e EC2. As sessões da VPC também são criptografadas.

Segurança da informação		IS-28.2	Vocês utilizam metadologias de criptografia aberta sempre que seus componentes de infraestrutura precisam se comunicar utilizando redes públicas (p. ex., replicação de dados baseada na Internet de um ambiente para outro)?	O Amazon S3 também oferece criptografia por parte do servidor como uma opção para os clientes. Os clientes também podem usar tecnologias de criptografia de terceiros. Consulte o whitepaper de visão geral de processos de segurança da AWS para obter detalhes adicionais - consulte em http://aws.amazon.com/pt/security.
Segurança da informação	Acesso a ferramentas de auditoria	IS-29.1	Vocês restringem, registram e monitoram o acesso aos seus sistemas de gerenciamento de segurança da informação (p. ex., hipervisores, firewalls, verificadores de vulnerabilidade, sniffers de rede, APIs, etc.)?	Em alinhamento com os padrões ISO 27001, a AWS estabeleceu procedimentos e políticas formais para delinear os padrões mínimos para acesso lógico a recursos da AWS. O relatório SOC 1, tipo II, da AWS descreve os controles vigentes para gerenciar o provisionamento a recursos da AWS. Consulte o whitepaper de visão geral de processos de segurança da AWS para obter detalhes adicionais - consulte em http://aws.amazon.com/pt/security.
Segurança da informação	Acesso a portas de configuração/ diagnóstico	IS-30.1	Vocês utilizam redes seguras dedicadas para fornecer acesso de gerenciamento à sua infraestrutura de serviço em nuvem?	Os administradores com uma necessidade de negócios de acessar o plano de gerenciamento são solicitados a usar a autenticação multifator para obter acesso aos hosts de uso específico de administração. Esses hosts administrativos são sistemas que são especificamente concebidos, criados, configurados e reforçados para proteger o plano de gerenciamento da nuvem. Todo esse acesso é registrado e auditado. Quando um funcionário não tem mais uma necessidade de negócio para acessar o plano de gestão, os privilégios e o acesso a esses hosts e sistemas pertinentes são revogados.
Segurança da informação	Serviços de infraestrutura/ rede	IS-31.1	Vocês coletam dados de capacidade e utilização para todos os componentes relevantes de sua oferta de serviço em nuvem?	A AWS gerencia dados de capacidade e utilização em alinhamento com o padrão ISO 27001. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Segurança da informação		IS-31.2	Vocês fornecem aos locatários relatórios de utilização e planejamento de capacidade?	
Segurança da informação	Dispositivos móveis/portáteis	IS-32.1	Há políticas e procedimentos estabelecidos e medidas implementadas para limitar rigidamente o acesso a dados confidenciais a partir de dispositivos móveis e portáteis, como laptops, celulares e PDAs, que geralmente apresentam risco superior a dispositivos não portáteis (p. ex., computadores desktop nas instalações da organização do provedor)?	Em alinhamento com padrões ISO 27001, a AWS estabeleceu procedimentos e políticas formais para delinear os padrões mínimos para acesso lógico a recursos da AWS. O relatório SOC 1, tipo II, da AWS descreve os controles vigentes para gerenciar o provisionamento de acesso a recursos da AWS. Consulte o whitepaper de visão geral de processos de segurança da AWS para obter detalhes adicionais - consulte em http://aws.amazon.com/pt/security.

Segurança da informação	Restrição de acesso a código-fonte	IS-33.1	Há controles vigentes para impedir o acesso não autorizado ao código-fonte de seu aplicativo, programa ou objeto e garantir que ele esteja restrito somente à equipe autorizada?	Em alinhamento com padrões ISO 27001, a AWS estabeleceu procedimentos e políticas formais para delinear os padrões mínimos para acesso lógico a recursos da AWS. O relatório SOC 1, tipo II, da AWS descreve os controles vigentes para gerenciar o provisionamento de acesso a recursos da AWS. Consulte o whitepaper de visão geral de processos de segurança da AWS para obter detalhes adicionais - consulte em http://aws.amazon.com/pt/security.
Segurança da informação		IS-33.2	Há controles vigentes para impedir o acesso não autorizado ao código-fonte do aplicativo, programa ou objeto do locatário e garantir que ele esteja restrito somente à equipe autorizada?	
Segurança da informação	Acesso a programas de utilitários	IS-34.1	Há utilitários que possam gerenciar significativamente partições virtualizadas (p. ex., desligamento, clone, etc.) devidamente restringidas e monitoradas?	Em alinhamento com os padrões ISO 27001, os utilitários do sistema são devidamente restringidos e monitorados. O relatório SOC 1, tipo II, da AWS fornece detalhes adicionais sobre controles vigentes para restringir o acesso ao sistema. Consulte o whitepaper de visão geral de processos de segurança da AWS para obter detalhes adicionais - consulte em http://aws.amazon.com/pt/security.
Segurança da informação		IS-34.2	Vocês têm recursos para detectar ataques que almejam a infraestrutura virtual diretamente (p. ex., "shimming", "Blue Pill", "Hyper jumping", etc.)?	
Segurança da informação		IS-34.3	Há ataques que almejam a infraestrutura virtual que sejam impedidos com controles técnicos?	
Legal	Acordos de confidencialidade	LG-01.1	Há requisitos para acordos de sigilo ou confidencialidade refletindo as necessidades da organização para a proteção de dados e detalhes operacionais identificados, documentados e revisados em intervalos planejados?	O departamento jurídico da Amazon gerencia e revisa periodicamente o acordo de confidencialidade da Amazon, a fim de refletir as necessidades comerciais da AWS.
Legal	Contratos de terceiros	LG-02.1	Vocês selecionam e monitoram provedores terceirizados em conformidade com legislações no país onde os dados são processados, armazenados e transmitidos?	A AWS não utiliza nenhum provedor de nuvem de terceiros para fornecer serviços da AWS para os clientes. Os contratos de terceiros são revisados pelo departamento jurídico da Amazon, conforme necessário.
Legal		LG-02.2	Vocês selecionam e monitoram provedores terceirizados em conformidade com legislações no país do qual os dados são originados?	
Legal		LG-02.3	O departamento jurídico revisa todos os contratos de terceiros?	
Gerenciamento de operações	Política	OP-01.1	Há políticas e procedimentos estabelecidos e disponibilizados para toda a equipe, a fim de oferecer suporte adequadamente às funções de operações de serviços?	Foram estabelecidos procedimentos e políticas pela estrutura de segurança da informação da AWS, com base na estrutura de COBIT, padrões do ISO 27001 e requisitos de PCI DSS. Consulte o whitepaper de conformidade e avaliação de riscos da AWS para obter detalhes adicionais - consulte em http://aws.amazon.com/pt/security.

Gerenciamento de operações	Documentação	OP-02.1	A documentação do sistema de informações (p. ex., guias do usuário e administrador, diagramas de arquitetura, etc.) é disponibilizada para a equipe autorizada, a fim de garantir a configuração, a instalação e a operação do sistema de informações?	A documentação do sistema de informações é disponibilizada internamente para a equipe da AWS através do uso do site da Intranet da Amazon. Consulte o whitepaper de visão geral de processos de segurança da AWS para obter detalhes adicionais - consulte em http://aws.amazon.com/pt/security.
Gerenciamento de operações	Planejamento de recursos/ capacidade	OP-03.1	Vocês fornecem documentação em relação a quais níveis de assinatura em excesso do sistema (rede, armazenamento, memória, E/S, etc.) são mantidos e em quais circunstâncias/cenários?	A AWS não divulga práticas de gerenciamento de capacidade. A AWS publica acordos de nível de serviço para serviços, a fim de comunicar comprometimentos de nível de desempenho.
Gerenciamento de operações		OP-03.2	Vocês restringem o uso das capacidades de assinatura em excesso de memória presentes no hipervisor?	
Gerenciamento de operações	Manutenção de equipamento	OP-04.1	Se estiver usando a infraestrutura virtual, sua solução em nuvem inclui capacidades de recuperação e restauração independentes de hardware?	A funcionalidade de snapshot do EBS permite que os clientes capturem e restaurem a qualquer momento imagens de máquina virtual. Os clientes podem exportar suas AMIs e usá-las localmente ou em outro provedor (sujeito a restrições de licenciamento de software). Consulte o whitepaper de visão geral de processos de segurança da AWS para obter detalhes adicionais - disponíveis em http://aws.amazon.com/pt/security.
Gerenciamento de operações		OP-04.2	Se estiver usando infraestrutura virtual, vocês fornecem locatários com uma capacidade de restaurar uma máquina virtual em um estado anterior específico no tempo?	
Gerenciamento de operações		OP-04.3	Se estiver usando infraestrutura virtual, vocês permitem que imagens de máquina virtual sejam baixadas e postadas em um novo provedor de nuvem?	
Gerenciamento de operações		OP-04.4	Se estiver usando infraestrutura virtual, imagens de máquina são disponibilizadas para o cliente, de forma que permita que o cliente replique essas imagens em seu próprio local de armazenamento fora do local?	
Gerenciamento de operações		OP-04.5	A sua solução de nuvem inclui capacidades de recuperação e restauração independentes de provedor/software?	
Gerenciamento de riscos	Programa	RI-01.1	A sua organização tem garantia de terceiros quanto a perdas?	A AWS fornece remuneração ao cliente por perdas que podem incorrer devido a interrupções no alinhamento com o acordo de nível de serviço da AWS.
Gerenciamento de riscos		RI-01.2	Os acordos de nível de serviço de sua organização fornecem remuneração a locatários por perdas que podem incorrer devido a interrupções ou perdas ocorridas em sua infraestrutura?	
Gerenciamento de riscos	Avaliações	RI-02.1	Há avaliações formais de risco alinhadas com a estrutura abrangendo toda a empresa e realizadas, pelo menos, anualmente ou em intervalos planejados, determinando a probabilidade e o impacto de todos os riscos identificados, usando métodos qualitativos e quantitativos?	Em alinhamento com o ISO 27001, a AWS desenvolveu um programa de gerenciamento de riscos para minimizar e gerenciar riscos. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.

Gerenciamento de riscos		RI-02.2	Existe a probabilidade e o impacto associados a riscos residuais e inerentes determinados de forma independente, considerando todas as categorias de risco (p. ex., resultados de auditoria, análise de vulnerabilidades/ameaças e conformidade normativa)?	Consulte o whitepaper de conformidade e avaliação de riscos da AWS (disponível em aws.amazon.com/pt/security) para obter mais detalhes sobre a estrutura de gerenciamento de riscos da AWS.
Gerenciamento de riscos	Minimização/ Aceitação	RI-03.1	Os riscos são minimizados para níveis aceitáveis com base em critérios estabelecidos pela empresa, de acordó com períodos de tempo de resolução razoáveis?	Em alinhamento com o padrão ISO 27001, Anexo A, domínio 4.2, a AWS desenvolveu um programa de gerenciamento de riscos para minimizar e gerenciar riscos. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001. Consulte o whitepaper de conformidade e avaliação de riscos da AWS (disponível em aws.amazon.com/pt/security) para obter mais detalhes sobre a estrutura de gerenciamento de riscos da AWS.
		RI-03.2	É realizada remediação em níveis aceitáveis com base em critérios estabelecidos pela empresa, de acordo com períodos de tempo razoáveis?	
Gerenciamento de riscos	Impactos de alterações de política/negócios	RI-04.1	Os resultados de avaliações de riscos incluem atualizações em controles, padrões, procedimentos e políticas de segurança, a fim de garantir que permaneçam pertinentes e eficazes?	As atualizações em controles, padrões, procedimentos e políticas de segurança da AWS ocorrem anualmente em alinhamento com o padrão ISO 27001. Consulte o ISO 27001, Anexo A, domínio 5.1 para obter mais informações. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Gerenciamento de riscos	Acesso de terceiros	RI-05.1	Vocês fornecem capacidade de recuperação de desastres no caso de várias falhas?	A AWS oferece aos clientes a flexibilidade de alocar instâncias e armazenar dados em várias regiões geográficas, bem como em várias zonas de disponibilidade dentro de cada região. Cada zona de disponibilidade é concebida como uma zona de falha independente. Em caso de falha, processos automatizados desviam o tráfego de dados do cliente da área afetada. Para obter mais detalhes, consulte o relatório SOC 1, tipo II, da AWS. O padrão ISO 27001, Anexo A, dominio 11, tipo II, fornece detalhes adicionais. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
		RI-05.2	Vocês monitoram a continuidade de serviço com provedores upstream na hipótese de falha do provedor?	
		RI-05.3	Vocês têm mais de um provedor para cada serviço com o qual contam?	
		RI-05.4	Vocês fornecem acesso a resumos de continuidade e redundância operacional, que incluem os serviços com os quais contam?	
		RI-05.5	Vocês fornecem ao locatário a capacidade de declarar um desastre?	
		RI-05.6	Vocês fornecem ao locatário uma opção de failover acionado?	
		RI-05.7	Vocês compartilham seus planos de redundância e continuidade de negócios com seus locatários?	

Gerenciamento de versões	Novo desenvolvimento/ aquisição	RM-01.1	Há políticas e procedimentos estabelecidos para autorização de gerenciamento para desenvolvimento ou aquisição de novos aplicativos, sistemas, bancos de dados, infraestrutura, serviços, operações e instalações?	Em alinhamento com os padrões ISO 27001, a AWS implementou procedimentos para gerenciar novo desenvolvimento de recursos. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001. Além disso, o relatório SOC 1, tipo II, da AWS fornece informações adicionais.
Gerenciamento de versões	Alterações em produção	RM-02.1	Vocês fornecem aos locatários documentação que descreve seus procedimentos de gerenciamento de alterações em produção, bem como suas funções/direitos/responsabilidades nela?	O relatório SOC 1, tipo II, da AWS fornece uma visão geral dos controles vigentes para gerenciar alterações no ambiente da AWS. Além disso, consulte o padrão ISO 27001, Anexo A, domínio 12.5 para obter mais detalhes. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Gerenciamento de versões	Testes de qualidade	RM-03.1	Vocês fornecem aos seus locatários documentação que descreve seu processo de garantia de qualidade?	A AWS incorpora padrões de qualidade como parte dos processos de SDLC (System Development Lifecycle, Ciclo de vida do desenvolvimento do sistema), que estão alinhados com o padrão ISO 27001. Consulte o padrão ISO 27001, Anexo A, dominio 10.1 para obter mais detalhes. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Gerenciamento de versões	Desenvolvimento terceirizado	RM-04.1	Vocês têm controles vigentes para garantir que padrões de qualidade estejam sendo atendidos para todo o desenvolvimento de software?	A AWS geralmente não terceiriza o desenvolvimento de software. A AWS incorpora padrões de qualidade como parte dos processos de SDLC, que estão alinhados com o padrão ISO 27001. Consulte o padrão ISO 27001, Anexo A, dominio 10.1 para obter mais detalhes. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Gerenciamento de versões		RM-04.2	Há controles vigentes para detectar defeitos de segurança de código-fonte para quaisquer atividades de desenvolvimento de software terceirizadas?	
Gerenciamento de versões	Instalações de software não autorizado	RM-05.1	Há controles vigentes para restringir e monitorar a instalação de software não autorizado em seus sistemas?	Os procedimentos, processos e programa da AWS para gerenciar software mal-intencionado estão em alinhamento com os padrões ISO 27001. Para obter mais detalhes, consulte o relatório SOC 1, tipo II, da AWS. Além disso, consulte o padrão ISO 27001, Anexo A, domínio 10.4 para obter mais detalhes. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.

Flexibilidade	Programa de gerenciamento	RS-01.1	Há políticas, processos e procedimentos definindo continuidade de negócios e recuperação de desastres vigentes para minimizar o impacto de um evento de risco detectado e comunicado devidamente aos locatários?	Os planos e políticas de continuidade de negócios da AWS foram desenvolvidos e testados em alinhamento com os padrões ISO 27001. Consulte o padrão ISO 27001, anexo A, dominio 14.1 e o relatório SOC 1, da AWS, para obter mais detalhes sobre a AWS e continuidade nos negócios.
Flexibilidade	Análise de impacto	RS-02.1	Vocês fornecem aos locatários relatórios e visibilidade contínua do desempenho de seu acordo de nível de serviço operacional?	O AWS CloudWatch oferece monitoramento de recursos em nuvem da AWS e de aplicativos que clientes executam na AWS. Para obter detalhes adicionais, consulte aws.amazon.com/cloudwatch. A AWS também publica nossas informações mais recentes sobre disponibilidade de serviço no Painel de saúde do serviço. Consulte status.aws.amazon.com.
Flexibilidade		RS-02.2	Há métricas de segurança da informação com base em padrões (CSA, CAMM, etc.) disponíveis para seus locatários?	
Flexibilidade		RS-02.3	Vocês fornecem aos clientes relatórios e visibilidade contínua do desempenho de seu acordo de nível de serviço operacional?	
Flexibilidade	Planejamento de continuidade nos negócios	RS-03.1	Vocês fornecem aos locatários opções de hospedagem flexíveis geograficamente?	Os datacenters são construídos em clusters em várias regiões globais. A AWS oferece aos clientes a flexibilidade de alocar instâncias e armazenar dados em várias regiões geográficas, bem como em várias zonas de disponibilidade dentro de cada região. Os clientes devem projetar seu uso da AWS para tirar proveito de várias regiões e zonas de disponibilidade. Consulte o whitepaper de visão geral de processos de segurança da AWS para obter detalhes adicionais - consulte em http://aws.amazon.com/pt/security.
Flexibilidade		RS-03.2	Vocês fornecem aos locatários capacidade de failover de serviço de infraestrutura para outros provedores?	
Flexibilidade	Testes de continuidade de negócios	RS-04.1	Há planos de continuidade de negócios sujeitos a testes em intervalos planejados ou mediante alterações ambientais ou organizações significativas, a fim de garantir a eficácia contínua?	Os planos de continuidade de negócios da AWS foram desenvolvidos e testados em alinhamento com os padrões ISO 27001. Consulte o padrão ISO 27001, anexo A, dominio 14.1 e relatório SOC 1, da AWS, para obter mais detalhes sobre a AWS e a continuidade de negócios.
Flexibilidade	Riscos ambientais	RS-05.1	Há proteção física em relação a danos de desastres e causas naturais, bem como ataques deliberados previstos, desenvolvidos e contramedidas aplicadas?	Os datacenters da AWS incorporam proteção física em relação a riscos ambientais. A proteção física da AWS em relação a riscos ambientais foi validada por um auditor independente e certificada como estando em alinhamento com as práticas recomendadas do ISO 27002. Consulte o padrão ISO 27001, anexo A, dominio 9.1 e relatório SOC 1, tipo II, da AWS, para obter mais informações.

Flexibilidade	Localização de equipamento	RS-06.1	Algum de seus datacenters localizados em lugares que tenham uma alta probabilidade/ocorrência de riscos ambientais de alto impacto (inundações, tornados, terremotos, furacões, etc.)?	Os datacenters da AWS incorporam proteção física em relação a riscos ambientais. Os serviços da AWS fornecem aos clientes a flexibilidade para armazenar dados em várias regiões geográficas, bem como em várias zonas de disponibilidade. Os clientes devem projetar seu uso da AWS para tirar proveito de várias regiões e zonas de disponibilidade. Consulte o padrão ISO 27001, anexo A, dominio 9.1 e relatório SOC 1, tipo II, da AWS, para obter mais informações.
Flexibilidade	Falhas de energia de equipamento	RS-07.1	Há redundâncias e mecanismos de segurança implementados para proteger equipamentos de interrupções de serviços públicos (p. ex., quedas de energia, interrupções de rede, etc.)?	O equipamento da AWS é protegido contra interrupções no alinhamento com o padrão ISO 27001. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001. O relatório SOC 1, tipo II, da AWS fornece detalhes adicionais sobre controles vigentes para minimizar o efeito de um mau funcionamento ou desastre físico no computador e em instalações de datacenter. Além disso, consulte o whitepaper de visão geral de processos de segurança - disponível em http://aws.amazon.com/pt/security.
Flexibilidade	Energia/ telecomunicações	RS-08.1	Vocês fornecem aos locatários documentação mostrando a rota de transporte de seus dados entre seus sistemas?	Os clientes da AWS determinam a região física em que seus dados e seus servidores estarão localizados. A AWS não moverá o conteúdo de clientes das Regiões selecionadas sem notificar o cliente, exceto se necessário para cumprir a legislação ou solicitações de entidades governamentais. Para obter mais detalhes, consulte o relatório SOC 1, tipo II, da AWS. Os clientes também podem escolher seu caminho de rede para instalações da AWS, incluindo em redes privadas e dedicadas, no qual o cliente controla o roteamento de tráfego.
Flexibilidade		RS-08.2	Os locatários podem definir como seus dados são transportados e por meio de qual jurisdição legal?	

Arquitetura de segurança	Exigências de acesso do cliente	SA-01.1	Todas as exigências normativas, contratuais e de segurança identificadas para acesso do cliente contratualmente atendidas e remediadas antes da concessão de acesso de clientes a dados, ativos e sistemas de informações?	Os clientes da AWS continuam com a responsabilidade de garantir que seu uso da AWS esteja em conformidade com regulamentos e legislações aplicáveis. A AWS comunica seu ambiente de controle e segurança para clientes através de declarações de terceiros e certificações, whitepapers (disponíveis em http://aws.amazon.com/pt/security) e fornecendo certificações, relatórios e outra documentação relevante diretamente para clientes da AWS. Consulte o padrão ISO 27001, Anexo A, dominio 6.2 para obter mais detalhes. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Arquitetura de segurança	Credenciais de ID de usuário	SA-02.1	Vocês oferecem suporte ao uso de, ou integração com, soluções existentes de logon único baseadas em cliente com seu serviço?	O serviço AWS Identity and Access Management (IAM) fornece federação de identidade para o AWS Management Console. A autenticação multifator é um recurso opcional que um cliente pode utilizar. Consulte o site da AWS para obter mais detalhes - http://aws.amazon.com/mfa.
Arquitetura de segurança		SA-02.2	Vocês usam padrões abertos para delegar recursos de autenticação aos seus locatários?	
Arquitetura de segurança		SA-02.3	Vocês oferecem suporte a padrões de federação de identidade (SAML, SPML, Federação WS, etc.) como uma forma de autenticar/autorizar usuários?	
Arquitetura de segurança		SA-02.4	Vocês têm uma capacidade de ponto de aplicação de política (p. ex., XACML), a fim de aplicar restrições de política e legais regionais em relação ao acesso do usuário?	
Arquitetura de segurança		SA-02.5	Vocês têm um sistema de gerenciamento de identidade vigente, que permita a qualificação com base em contexto e funções para dados (permite a classificação de dados para um locatário)?	
Arquitetura de segurança		SA-02.6	Vocês fornecem aos locatários opções rígidas de autenticação (multifator) (certificados digitais, tokens, biométrica, etc.) para acesso de usuário?	
Arquitetura de segurança		SA-02.7	Vocês permitem que os locatários usem serviços de garantia de identidade de terceiros?	
Arquitetura de segurança	Integridade/ segurança de dados	SA-03.1	A sua arquitetura de segurança de dados foi desenvolvida usando um padrão do setor (por exemplo, CDSA, MULITSAFE, padrão de arquitetura de nuvem confiável da CSA, FedRAMP CAESARS)?	A arquitetura de segurança de dados da AWS foi desenvolvida para incorporar práticas líderes do setor. Consulte o padrão ISO 27001, Anexo A, dominio 10.8 para obter mais detalhes. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.

Arquitetura de segurança	Segurança de aplicativo	SA-04.1	Vocês utilizam padrões do setor (comparações de BSIMM [Build Security in Maturity Model, Criação de segurança em modelo de maturidade], estrutura de provedor de tecnologia confiável de ACS de grupo aberto, etc.) para criar segurança para seu SDLC?	O ciclo de vida de desenvolvimento de sistema da AWS incorpora práticas recomendadas do setor, que incluem revisões formais de design pela equipe de segurança da AWS, modelagem de ameaças e conclusão de uma avaliação de risco. Consulte a visão geral de processos de segurança da AWS para obter mais detalhes. Além disso, consulte o padrão ISO 27001, Anexo A, domínio 12.5 para obter mais detalhes. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Arquitetura de segurança		SA-04.2	Vocês utilizam uma ferramenta de análise de código-fonte automatizada para detectar defeitos de segurança de código antes da produção?	
Arquitetura de segurança		SA-04.3	Vocês verificam se todos os fornecedores de software seguem os padrões do setor para segurança de SDLC?	
Arquitetura de segurança	Integridade de dados	SA-05.1	Há rotinas de integridade de entrada e saída de dados (ou seja, verificações de edições e reconciliação) implementadas para bancos de dados e interfaces de aplicativos, a fim de prevenir corrupção de dados ou erros de processamento sistemático ou manual?	Os controles de integridade de dados da AWS, como descrito no relatório SOC 1, tipo II, da AWS, fornecem garantia razoável de que a integridade de dados será mantida em todas as fases, incluindo transmissão, armazenamento e processamento. Além disso, consulte o padrão ISO 27001, Anexo A, domínio 12.2 para obter mais informações. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Arquitetura de segurança	Ambientes de produção/não produção	SA-06.1	Para sua oferta SaaS ou PaaS, vocês fornecem aos locatários ambientes separados para processos de teste e produção?	Os clientes da AWS mantêm a capacidade e a responsabilidade por criar e manter ambientes de produção e teste. O site da AWS fornece orientações sobre a criação de um ambiente utilizando os serviços da AWS - http://aws.amazon.com/documentation/.
Arquitetura de segurança		SA-06.2	Para sua oferta IaaS, vocês fornecem aos locatários orientações sobre como criar ambientes adequados de produção e teste?	
Arquitetura de segurança	Autenticação multifator de usuário remoto	SA-07.1	A autenticação multifator é necessária para todo o acesso de usuário remoto?	A autenticação multifator é um recurso opcional que um cliente pode utilizar. Consulte o site da AWS para obter mais detalhes - http://aws.amazon.com/mfa.
Arquitetura de segurança	Segurança de rede	SA-08.1	Para sua oferta IaaS, vocês fornecem aos clientes orientações sobre como criar uma arquitetura de segurança em camadas equivalente usando sua solução virtualizada?	O site fornece orientações sobre como criar uma arquitetura de segurança em camadas em vários whitepapers, disponíveis nosite público da AWS - http://aws.amazon.com/documentation/.
Arquitetura de segurança	Segmentação	SA-09.1	Há ambientes de rede e sistema logicamente separados, a fim de garantir os requisitos de segurança comercial e do cliente?	Os clientes da AWS continuam tendo responsabilidade por gerenciar sua própria segmentação de rede em adesão com seus requisitos definidos. Internamente, a segmentação de rede da AWS está alinhada com os padrões ISO 27001. Consulte o padrão ISO 27001, Anexo A, dominio 11.4 para obter mais detalhes.
Arquitetura de segurança		SA-09.2	Há ambientes de rede e sistema logicamente separados, a fim de garantir a conformidade com requisitos legislativos, normativos e contratuais?	

Arquitetura de segurança		SA-09.3	Há ambientes de rede e sistema logicamente separados, a fim de garantir a separação de ambientes de produção e não produção?	A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Arquitetura de segurança		SA-09.4	Há ambientes de rede e sistema logicamente separados, a fim de garantir a proteção e o isolamento de dados confidenciais?	
Arquitetura de segurança	Segurança sem fio	SA-10.1	Há políticas e procedimentos estabelecidos e mecanismos implementados, a fim de proteger o parâmetro de ambiente de rede, e configurados para restringir o tráfego não autorizado?	Há políticas, procedimentos e mecanismos para proteger o ambiente de rede da AWS. Para obter mais detalhes, consulte o relatório SOC 1, tipo II, da AWS. Além disso, consulte o padrão ISO 27001, Anexo A, domínio 10.6 para obter mais informações. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Arquitetura de segurança		SA-10.2	Há políticas e procedimentos estabelecidos e mecanismos implementados, a fim de garantir que as configurações apropriadas de segurança estejam habilitadas com rígida criptografia para autenticação e transmissão, substituindo configurações padrão de fornecedor (p. ex., chaves de criptografia, senhas, sequência de caracteres de comunidade de SNMP, etc.)?	
Arquitetura de segurança		SA-10.3	Há políticas e procedimentos estabelecidos e mecanismos implementados, a fim de proteger ambientes de rede e detectar a presença de dispositivos de rede não autorizados (invasores) para uma desconexão da rede em tempo hábil?	
Arquitetura de segurança	Redes compartilhadas	SA-11.1	O acesso a sistemas com infraestrutura de rede compartilhada está restrito à equipe autorizada, de acordo com padrões, procedimentos e políticas de segurança. As redes compartilhadas com entidades externas deverão ter um plano documentado detalhando os controles de compensação usados, a fim de separar o tráfego de rede entre organizações?	O acesso é estritamente restrito a recursos essenciais, incluindo serviços, hosts e dispositivos de rede, e deve ser explicitamente aprovado no sistema de gerenciamento de permissões de propriedade da Amazon. O relatório SOC 1, tipo II, da AWS fornece detalhes adicionais sobre atividades específicas de controle executadas pela AWS. Além disso, consulte o padrão ISO 27001, Anexo A, domínio 11. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Arquitetura de segurança	Sincronização de relógio	SA-12.1	Não utilize um protocolo de serviço com tempo sincronizado (p. ex., NTP), a fim de garantir que todos os sistemas tenham uma referência de horário comum?	Em alinhamento com os padrões do ISO 27001, os sistemas de informação da AWS utilizam relógios do sistema interno sincronizados via NTP (Network Time Protocol, Protocolo de horário de rede). A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.

Arquitetura de segurança	Identificação de equipamento	SA-13.1	A identificação de equipamento automatizado é usada como um método de autenticação de conexão, a fim de validar a integridade de autenticação da conexão com base em local de equipamento conhecido?	A AWS gerencia a identificação de equipamento em alinhamento com o padrão ISO 27001. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Arquitetura de segurança	Detecção de intrusão/registro em log de auditoria	SA-14.1	Há ferramentas de IDS (detecção de intrusão de rede) e integridade de arquivo (host) implementadas para ajudar a facilitar a detecção em tempo hábil, a investigação por análise de causa raiz e a resposta a incidentes?	O programa de resposta a incidentes da AWS (detecção, investigação e resposta a incidentes) foi desenvolvido em alinhamento com o padrão ISO 27001. O relatório SOC 1, tipo II, da AWS fornece detalhes sobre atividades específicas de controle executadas pela AWS. O whitepaper de visão geral de processos de segurança da AWS (disponível em http://aws.amazon.com/pt/security) fornece detalhes adicionais.
Arquitetura de segurança		SA-14.2	Há acesso de usuário lógico e físico para auditar logs restritos à equipe autorizada?	
Arquitetura de segurança		SA-14.3	Vocês podem fornecer evidências de que o mapeamento de auditoria detalhada de regulamentos e padrões em seus controles/arquitetura/processos foi feito?	
Arquitetura de segurança	Código para dispositivo móvel	SA-15.1	O código para dispositivo móvel é autorizado antes de sua instalação e uso? A configuração do código é verificada para garantir que o código para dispositivo móvel autorizado opera de acordo com uma política de segurança claramente definida?	A AWS permite aos clientes gerenciar os aplicativos móveis e clientes para suas próprias necessidades.
Arquitetura de segurança		SA-15.2	Todos os códigos para dispositivos móveis não autorizados têm sua execução impedida?	

APÊNDICE B – GLOSSÁRIO DE TERMOS

Acordo de nível de serviço (SLA): é a parte de um acordo de serviço onde o nível de serviço é formalmente definido. O SLA é usado para referir-se ao tempo de entrega contratado (do serviço) ou desempenho.

Autenticação: a autenticação é o processo de determinar se alguém ou alguma coisa é realmente quem ou o que ele declara ser.

DSS: o padrão de segurança de dados do setor de cartão de pagamento (DSS) é um padrão mundial de segurança da informação criado e gerenciado pelo Conselho de padrões de segurança de dados do setor de cartão de pagamento.

EBS: o Amazon Elastic Block Store (EBS) fornece volumes de armazenamento em bloco para uso com instâncias do Amazon EC2. Os volumes do Amazon EBS são armazenamentos fora da instância que persistem independentemente da duração de uma instância.

FIPS 140-2: a publicação do FIPS (Federal Information Processing Standard, Padrão federal de processamento de informações) 140-2 é um padrão de segurança do governo dos EUA que especifica os requisitos de segurança para módulos criptográficos protegendo informações confidenciais.

FISMA: Federal Information Security Management Act de 2002. A lei exige que cada agência federal desenvolva, documente e implemente um programa em toda a agência, a fim de fornecer a segurança para as informações e sistemas que oferecem suporte a operações e ativos da agência, incluindo aqueles fornecidos ou gerenciados por outra agência, contratante ou de outra fonte.

GLBA: a Gramm-Leach-Bliley Act (GLB ou GLBA), também conhecida como a Lei de modernização de serviços financeiros de 1999, estabelece requisitos para instituições financeiras com relação à, entre outras coisas, divulgação de informações confidenciais dos clientes e a proteção das ameaças à integridade de dados e segurança.

HIPAA: a Health Insurance Portability e Accountability Act (Lei da Portabilidade e Prestação de Contas em Seguro Saúde, HIPAA) de 1996, exige o estabelecimento de normas nacionais para transações eletrônicas de cuidados de saúde e identificadores nacionais para provedores, planos de saúde e empregadores. As disposições de simplificação de administração também abordam a segurança e a privacidade dos dados de saúde. As normas são destinadas a melhorar a eficiência e a eficácia do sistema de saúde do país, incentivando o uso generalizado de transferência eletrônica de dados no sistema de cuidados de saúde dos EUA.

Hipervisor: um hipervisor, também chamado de Monitor de máquina virtual (VMM), é um software de virtualização de plataforma de hardware/software que permite que vários sistemas operacionais sejam executados simultaneamente em um computador host.

IAM: o AWS Identity and Access Management (IAM) permite que você crie múltiplos usuários e gerencie permissões para cada um desses usuários a partir de sua conta da AWS.

Instância virtual: uma vez que uma AMI seja executada, o sistema resultante em execução é referido como uma instância. Todas as instâncias baseadas na mesma AMI iniciam idênticas e qualquer informação sobre elas é perdida quando as instâncias são concluídas ou na ocorrência de falhas.

ISAE 3402: as Normas internacionais para contratos de garantia nº 3402 (ISAE 3402) são o padrão internacional sobre contratos de garantia. Ela foi aplicada pelo International Auditing and Assurance Standards Board (IAASB), um comitê de definição de pdarões na International Federation of Accountants (IFAC). O ISAE 3402 é agora o novo padrão reconhecido globalmente para relatórios de garantias em empresas de serviços.

ISO 27001: o ISO/IEC 27001 é um padrão do Information Security Management System (Sistema de gerenciamento de segurança da informação, ISMS), publicado pela International Organization for Standardization (Organização internacional para padronização, ISO) e International Electrotechnical Commission (Comissão eletrotécnica internacional, IEC). O ISO 27001 especifica formalmente um sistema de gestão que destina-se a fornecer segurança da informação sob o controle de gerenciamento explícito. Sendo um meio de especificação formal, exige requisitos específicos. As organizações que alegam ter adotado o ISO/IEC 27001 podem, portanto, ser auditadas e certificadas em conformidade com o padrão.

ITAR: International Traffic in Arms Regulations ou Regulamentos sobre tráfico internacional de armas é um conjunto de regulamentos do governo dos EUA, que controlam a exportação e a importação de artigos relacionados à defesa e serviços na United States Munitions List (USML). As agências governamentais e contratantes devem cumprir os ITAR e restringir o acesso a dados protegidos.

NIST: National Institute of Standards and Technology (Instituto nacional de normas e tecnologia). Esta agência define normas detalhadas de segurança conforme necessário para programas do setor ou do governo. A conformidade com a FISMA exige que agências sigam padrões NIST.

Objeto: entidades fundamentais armazenadas no Amazon S3. Os objetos consistem em metadados e dados de objeto. A porção de dados é opaca para o AmazonS3. Os metadados são um conjunto de pares de nome e valor que descrevem o objeto. Estes incluem alguns metadados padrão tais como a data da última modificação e metadados HTTP padrão como Content-Type. O desenvolvedor também pode especificar metadados personalizados no momento em que o objeto é armazenado.

PCI: refere-se ao Conselho de padrão de segurança do setor de cartão de pagamento, um Conselho independente formado pela American Express, Discover Financial Services, JCB, MasterCard Worldwide e Visa International, com o objetivo de gerenciar a contínua evolução do padrão de segurança de dados do setor de cartão de pagamento.

QSA: a designação de Qualified Security Assessor (Assessor de segurança qualificado, QSA) é conferida pelo PCI Security Standards Council aos indivíduos que atendem aos requisitos de qualificação específica e estão autorizados a efetuar avaliações de conformidade com PCI.

SAS 70: declaração sobre as normas de auditoria n° 70: empresas de serviços é uma instrução de auditoria emitida pelo Auditing Standards Board do American Institute of Certified Public Accountants (AICPA). O SAS 70 fornece orientação para auditores de serviço ao avaliarem os controles internos de uma empresa de serviços (tais como a AWS) e emitirem um relatório de auditoria de um serviço. O SAS 70 também fornece orientação para auditores de demonstrativos financeiros de uma entidade que usa uma ou mais empresas de serviços. O relatório SAS 70 foi substituído pelo relatório SOC 1.

Serviço: capacidade de computação ou software fornecido através de uma rede (por exemplo, EC2, S3, VPC, etc.).

SOC 1: relatório Service Organization Controls 1 (SOC 1), tipo II, anteriormente chamado de relatório Statement on Auditing Standards (SAS) No. 70, empresas de serviços (comumente referido como o relatório SSAE 16), é um padrão de auditoria amplamente reconhecido, desenvolvido pelo American Institute of Certified Public Accountants (AICPA). O padrão internacional é referido como o International Standards for Assurance Engagements No. 3402 (ISAE 3402).

SSAE 16: O Statement on Standards for Attestation Engagements No. 16 (SSAE 16) é um padrão de declaração publicado pelo Auditing Standards Board (ASB) do American Institute of Certified Public Accountants (AICPA). O padrão atende a contratos realizados por um auditor de serviço para relatórios sobre controles em organizações que fornecem serviços a entidades de usuários, para as quais os controles da empresa de serviços provavelmente serão relevantes para um controle interno de entidades de usuário em relatórios financeiros (ICFR). O SSAE 16 substitui eficazmente o Statement on Auditing Standards No. 70 (SAS 70) para períodos de relatórios de auditor de serviços encerrando em 15 de junho de 2011 ou posteriormente.

Zona de disponibilidade: os locais do Amazon EC2 são compostos pelas regiões e pelas Zonas de disponibilidade. As Zonas de disponibilidade são as posições distintas que são projetadas para serem isoladas das falhas em outras Zonas da disponibilidade e fornecem rede de conectividade acessível e de baixa latência para outras Zonas de disponibilidade da mesma região.

Versão de julho de 2012

- Edições em conteúdo e escopo de certificação atualizado
- Acréscimo do CSA Consensus Assessments Initiative Questionnaire (Apêndice A)

Versão de janeiro de 2012

- Pequenas edições em conteúdo com base no escopo de certificação atualizado
- Pequenas correções gramaticais

Versão de dezembro de 2011

- Alteração na seção de declaração de terceiros e certificações para refletir SOC 1/SSAE 16, FISMA, nível moderado, regulamentos sobre o tráfico internacional de armas e FIPS 140-2
- Acréscimo da criptografia de servidor do S3
- Tópicos adicionais da questão de computação em nuvem adicionados

Versão de maio de 2011
Versão inicial

Avisos