Questionário da iniciativa de avaliação de consenso da CSA

Janeiro de 2017

Avisos

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

Índice

Resumo

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 utilizadas de várias formas, incluindo avaliação de segurança e seleção de provedor de nuvem. A AWS concluiu esse questionário com as respostas a seguir.

Introdução

A Cloud Security Alliance (CSA) é uma "organização sem fins lucrativos, com a missão de promover o uso das melhores práticas 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." Para obter mais informações, consulte https://cloudsecurityalliance.org/about/.

Uma ampla variedade de associações, corporações e pessoas do setor de segurança participam desta organização para cumprir sua missão.

Questionário da iniciativa de avaliação de consenso da CSA

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Segurança de aplicações e interface *Segurança de aplicações*	AIS-01.1	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. A AWS implementou procedimentos para gerenciar novos desenvolvimentos de recursos. Consulte o padrão ISO 27001, Anexo A, domínio 14 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.
	AIS-01.2	Vocês utilizam uma ferramenta de análise de código-fonte automatizada para detectar defeitos de segurança no código antes da produção?	
	AIS-01.3	Vocês utilizam uma ferramenta de análise de código-fonte manual para detectar defeitos de segurança no código antes da produção?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	AIS-01.4	Vocês verificam se todos os fornecedores de software seguem os padrões do setor para segurança de SDLC?	
	AIS-01.5	(Apenas SaaS) Vocês revisam suas aplicações para evitar vulnerabilidades de segurança e resolver quaisquer problemas antes da implantação para a produção?	
Segurança de aplicações e interface *Exigências de acesso do cliente*	AIS-02.1	Todas as exigências normativas, contratuais e de segurança identificadas para acesso do cliente contratualmente foram 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/compliance) e fornecendo certificações, relatórios e outros documentos relevantes diretamente para clientes da AWS.
	AIS- 02.2	Será que todos os requisitos e níveis de confiança para o acesso dos clientes estão definidos e documentados?	
Segurança de aplicações e interface *Integridade de dados*	AIS-03.1	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 aplicações, 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 da AWS, ilustram os controles da integridade de dados mantidos em todas as fases, incluindo transmissão, armazenamento e processamento. Além disso, consulte o padrão ISO 27001, Anexo A, domínio 14 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.

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Segurança de aplicações e interface *Integridade/ segurança de dados*	AIS-04.1	Sua arquitetura de segurança de dados é projetada usando um padrão da indústria (por exemplo, CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	A arquitetura de segurança de dados da AWS foi desenvolvida para incorporar práticas líderes do setor. Consulte Certificações, relatórios e whitepapers da AWS para obter mais detalhes sobre as várias práticas de liderança às quais a AWS adere (disponível em http://aws.amazon.com/compliance).
Controle de auditoria e conformidade *Planejamento de auditoria*	AAC-01.1	Vocês produzem declarações de auditoria usando um formato estruturado e aceito pelo setor (por exemplo, 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 outros documentos relevantes para clientes da AWS (acordo de confidencialidade).
Controle de auditoria e conformidade *Auditorias independentes*	AAC-02.1	Vocês permitem que grupos de usuários vejam seus relatórios SOC2/ISO 27001 ou relatórios de auditoria ou certificação de terceiros semelhantes?	A AWS fornece declarações de terceiros, certificações, relatórios de controles de empresa de serviços (SOC) e outros relatórios de conformidade relevantes diretamente para nossos clientes sob o NDA. É possível baixar a certificação ISO 27001 da AWS aqui. O relatório AWS SOC 3 pode ser baixado aqui. A segurança da AWS examina regularmente todos os endereços IP de endpoint de serviço voltados 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.
	AAC-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?	
	AAC-02.3	Vocês executam testes de penetração de aplicações na sua infraestrutura em nuvem regularmente, conforme indicado pelas práticas recomendadas e orientações do setor?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	AAC-02.4	Vocês realizam regularmente auditorias internas, como prescrito pelas orientações e práticas recomendadas do setor?	Além disso, o ambiente de controle da AWS está sujeito a avaliações de risco e auditorias internas e externas regulares. A AWS contrata órgãos externos de certificação e auditores independentes para analisar e testar o ambiente de controle geral da AWS.
	AAC-02.5	Vocês realizam regularmente auditorias externas, como prescrito pelas orientações e práticas recomendadas do setor?	
	AAC-02.6	Os resultados de testes de penetração estão disponíveis para grupos de usuários mediante solicitação?	
	AAC-02.7	Os resultados de auditorias internas e externas estão disponíveis para grupos de usuários mediante solicitação?	
	AAC-02.8	Vocês têm um programa de auditoria interna que permite a auditoria entre funções das avaliações?	
Controle de auditoria e conformidade *Mapeamento normativo do sistema de informações*	AAC-03.1	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 grupo de usuários, sem acessar inadvertidamente os dados de outro grupo?	Todos os dados armazenados pela AWS em nome dos clientes têm recursos sólidos de segurança e controle de isolamento de grupos de usuários. 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. Os túneis IPSec para a VPC também são criptografados. Além disso, os clientes podem aproveitar o AWS Key Management Systems (KMS) para criar e controlar chaves de criptografia (consulte https://aws.amazon.com/kms/). Consulte o Whitepaper de Segurança na Nuvem AWS para obter detalhes adicionais, disponível em http://aws.amazon.com/security

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	AAC-03.2	Vocês têm capacidade para recuperar logicamente dados de um cliente específico no caso de uma falha ou perda de dados?	A AWS permite que clientes executem seus backups usando seu próprio provedor de serviço de backup em unidades de fita. No entanto, um backup em fita não é um serviço prestado pela AWS. Os serviços Amazon S3 e Glacier são projetados para conduzir a probabilidade de perda de dados para perto de zero por cento e a durabilidade equivalente das cópias multissite de objetos de dados é conseguida através de redundância de armazenamento de dados. Para obter informações sobre durabilidade e redundância de dados, consulte o website da AWS.
	AAC-03.3	Vocês têm a capacidade de restringir o armazenamento de dados do cliente a determinados países ou localizações geográficas?	Os clientes da AWS podem designar em qual região física seu conteúdo estará localizado. A AWS não moverá o conteúdo de clientes das regiões selecionadas sem notificá-los, exceto se necessário para cumprir a legislação ou atender a solicitações de entidades governamentais. Para ver uma lista completa das regiões disponíveis, consulte a página Infraestrutura global da AWS.
	AAC-03.4	Vocês têm um programa local que inclui a capacidade de monitorar mudanças nos requisitos regulamentares em jurisdições relevantes, ajustar o seu programa de segurança para alterações em requisitos legais e garantir a conformidade com os requisitos regulamentares relevantes?	A AWS monitora os requisitos legais e regulamentares pertinentes. Consulte a norma ISO 27001 Anexo 18 para obter detalhes adicionais. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Gerenciamento de continuidade de negócios e resiliência operacional *Planejamento de continuidade nos negócios*	BCR-01.1	Vocês fornecem a grupos de usuários opções de hospedagem flexíveis geograficamente?	Os datacenters são construídos em clusters em várias regiões globais. A AWS oferece aos clientes a flexibilidade de posicionar 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 Segurança na Nuvem da AWS para obter detalhes adicionais, disponível em http://aws.amazon.com/security.
	BCR-01.2	Vocês fornecem a grupos de usuários capacidade de failover de serviço de infraestrutura para outros provedores?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Gerenciamento de continuidade de negócios e resiliência operacional *Testes de continuidade de negócios*	BCR-02.1	Há planos de continuidade de negócios sujeitos a testes em intervalos planejados ou mediante alterações ambientais ou organizacionais significativas, a fim de garantir a eficácia contínua?	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, domínio 17 para obter mais detalhes sobre a AWS e a continuidade de negócios.
Gerenciamento de continuidade de negócios e resiliência operacional *Energia/teleco-municações*	BCR-03.1	Vocês fornecem a grupos de usuários 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 servidores estarão localizados. A AWS não moverá o conteúdo de clientes das regiões selecionadas sem notificá-los, exceto se necessário para cumprir a legislação ou atender a solicitações de entidades governamentais. Para obter mais detalhes, consulte o relatório SOC da AWS. Os clientes também podem escolher seu caminho de rede para instalações da AWS, incluindo em redes privadas e dedicadas, onde o cliente controla o roteamento de tráfego.
	BCR-03.2	Grupos de usuários podem definir como seus dados são transportados e por meio de quais jurisdições legais?	
Gerenciamento de continuidade de negócios e resiliência operacional Documentação	BCR-04.1	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 Segurança na Nuvem AWS para obter detalhes adicionais, disponível em http://aws.amazon.com/security/. Consulte a ISO 27001, Apêndice A, domínio 12.
Gerenciamento de continuidade de negócios e resiliência operacional *Riscos ambientais*	BCR-05.1	Há proteção física em relação a danos (por exemplo, desastres e causas naturais e ataques deliberados) previstos e desenvolvidos com contramedidas aplicadas?	Os datacenters da AWS incorporam proteção física contra 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, domínio 11.

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Gerenciamento de continuidade de negócios e resiliência operacional *Localização de equipamento*	BCR-06.1	Algum de seus datacenters está localizado em lugares que tenham alta probabilidade/ocorrência de riscos ambientais de alto impacto (inundações, tornados, terremotos, furacões etc.)?	Os datacenters da AWS incorporam proteção física contra 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, domínio 11.
Gerenciamento de continuidade de negócios e resiliência operacional *Manutenção de equipamento*	BCR-07.1	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 Segurança na Nuvem AWS para obter detalhes adicionais, disponível em http://aws.amazon.com/security.
	BCR-07.2	Se estiver usando infraestrutura virtual, vocês fornecem a grupos de usuários a capacidade de restaurar uma máquina virtual em um estado anterior específico no tempo?	
	BCR-07.3	Se estiver usando infraestrutura virtual, vocês permitem que imagens de máquina virtual sejam baixadas e postadas em um novo provedor de nuvem?	
	BCR-07.4	Se estiver usando infraestrutura virtual, imagens de máquina serão disponibilizadas para o cliente, de forma que ele possa replicar essas imagens em seu próprio local de armazenamento fora do local?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	BCR-07.5	Sua solução de nuvem inclui recursos de recuperação e restauração independentes de provedor/software?	
Gerenciamento de continuidade de negócios e resiliência operacional *Falhas de energia de equipamento*	BCR-08.1	Há redundâncias e mecanismos de segurança implementados para proteger equipamentos de interrupções de serviços públicos (por exemplo, quedas de energia, interrupções de rede, etc.)?	O equipamento da AWS é protegido contra interrupções de serviços públicos de acordo com a norma ISO 27001. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001. Os relatórios SOC da AWS fornecem detalhes adicionais sobre controles vigentes para minimizar o efeito de um mau funcionamento ou desastre físico no computador e nas instalações do datacenter. Além disso, consulte o Whitepaper de Segurança na Nuvem da AWS, disponível em http://aws.amazon.com/security.
Gerenciamento de continuidade de negócios e resiliência operacional *Análise de impacto*	BCR-09.1	Vocês fornecem a grupos de usuários 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 aplicações que clientes executam na AWS. Consulte aws.amazon.com/cloudwatch para obter detalhes adicionais. A AWS também publica nossas informações mais recentes sobre disponibilidade de serviço no Painel de Status dos Serviços. Consulte status.aws.amazon.com.
	BCR-09.2	Há métricas de segurança da informação com base em padrões (CSA, CAMM etc.) disponíveis para seus grupos de usuários?	
	BCR-09.3	Vocês fornecem aos clientes relatórios e visibilidade contínua do desempenho de seu acordo de nível de serviço operacional?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Gerenciamento de continuidade de negócios e resiliência operacional *Política*	BCR-10.1	Há políticas e procedimentos estabelecidos e disponibilizados para toda a equipe, a fim de oferecer adequadamente suporte às funções de operações de serviços?	Foram estabelecidos procedimentos e políticas pela estrutura de segurança da AWS, com base nas normas NIST 800-53, ISO 27001, ISO 27017, ISO 27018, ISO 9001 e nos requisitos de PCI DSS. Consulte o Whitepaper de Conformidade e Avaliação de Riscos da AWS para obter mais detalhes, disponível em http://aws.amazon.com/compliance.
Gerenciamento de continuidade de negócios e resiliência operacional *Política de retenção*	BCR-11.1	Vocês têm recursos de controle técnico para aplicar políticas de retenção de dados de grupo de usuários?	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 Segurança na Nuvem AWS para obter detalhes adicionais, disponível em http://aws.amazon.com/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 contestar ordens legais se acreditar que elas sejam infundadas ou não possuam embasamento sólido. Para obter informações adicionais, consulte https://aws.amazon.com/compliance/data-privacy-faq/.
	BCR-11.2	Vocês têm um procedimento documentado para responder a solicitações de dados de grupos de usuários de governos ou terceiros?	
	BCR-11.4	Vocês implementaram mecanismos de backup ou redundância para garantir a conformidade com requisitos normativos, estatutários, contratuais ou comerciais?	Os mecanismos de backup e redundância da AWS foram desenvolvidos e testados de acordo com as normas ISO 27001. Consulte a norma ISO 27001, anexo A, domínio 12 e o relatório SOC 2, da AWS, para obter informações adicionais sobre os mecanismos de backup e redundância da AWS.
	BCR-11.5	Vocês testam seus mecanismos de backup ou redundância pelo menos uma vez por ano?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Controle de mudanças e gerenciamento de configurações *Novo desenvolvi-mento/ aquisição*	CCC-01.1	Há políticas e procedimentos estabelecidos para autorização de gerenciamento para desenvolvimento ou aquisição de novas aplicações, sistemas, bancos de dados, infraestrutura, serviços, operações e instalações?	Foram estabelecidos procedimentos e políticas pela estrutura de segurança da AWS, com base nas normas NIST 800-53, ISO 27001, ISO 27017, ISO 27018, ISO 9001 e nos requisitos de PCI DSS. Independentemente de o cliente ser novo na AWS ou um usuário avançado, informações úteis sobre os serviços, desde apresentações a recursos avançados, estão disponíveis na seção Documentação da AWS do nosso site em https://aws.amazon.com/documentation/.
	CCC-01.2	Existe alguma documentação disponível que descreva a instalação, a configuração e o uso de produtos/ serviços/recursos?	
Controle de mudanças e gerenciamento de configurações *Desenvolvi-mento terceirizado*	CCC-02.1	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 (ciclo de vida de desenvolvimento do sistema). Consulte o padrão ISO 27001, Anexo A, domínio 14 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.
	CCC-02.2	Há controles vigentes para detectar defeitos de segurança de código-fonte para quaisquer atividades de desenvolvimento de software terceirizadas?	
Controle de mudanças e gerenciamento de *configurações* *Testes de qualidade*	CCC-03.1	Vocês fornecem a seus grupos de usuários documentação que descreve seu processo de garantia de qualidade?	A AWS mantém uma certificação ISO 9001. Trata-se de uma validação independente do sistema de qualidade da AWS que determina se as atividades da AWS estão em conformidade com os requisitos do ISO 9001. Os boletins de segurança da AWS notificam os clientes sobre eventos de segurança e privacidade. Os clientes podem se inscrever no feed RSS do boletim de segurança da AWS no nosso site. Consulte aws.amazon.com/security/security-bulletins/.
	CCC-03.2	Existe alguma documentação disponível que descreva problemas conhecidos com alguns produtos/serviços?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	CCC-03.3	Existem políticas e procedimentos em vigor para analisar e corrigir bugs e vulnerabilidades de segurança relatados para produtos e serviços?	A AWS também publica nossas informações mais recentes sobre disponibilidade de serviço no Painel de Status dos Serviços. Consulte status.aws.amazon.com. O ciclo de vida de desenvolvimento de sistema da AWS (SDLC) incorpora as melhores práticas 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 14 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.
	CCC-03.4	Existem mecanismos em vigor para garantir que todos os elementos de depuração e código de teste sejam removidos das versões de software lançadas?	
Controle de mudanças e gerenciamento de configurações *Instalações de software não autorizado*	CCC-04.1	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. Consulte o padrão ISO 27001, Anexo A, domínio 12 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.
Controle de mudanças e gerenciamento de configurações *Alterações em produção*	CCC-05.1	Vocês fornecem a grupos de usuários documentação que descreve seus procedimentos de gerenciamento de alterações em produção, bem como suas funções/direitos/ responsabilidades?	Os relatórios SOC da AWS fornecem uma visão geral dos controles vigentes para gerenciar alterações no ambiente da AWS. Além disso, consulte o padrão ISO 27001, Anexo A, domínio 12 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.

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Segurança de dados e gerenciamento do ciclo de vida das informações *Classificação*	DSI-01.1	Vocês fornecem algum recurso para identificar máquinas virtuais por meio de tags/metadados de política (por exemplo, tags podem ser usadas para limitar sistemas operacionais convidados de inicializar/instanciar/ transportar dados no país errado)?	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.
	DSI-01.2	Vocês fornecem recursos para identificar hardware via tags/metadados/tags de hardware de política (por exemplo, TXT/TPM, VN-Tag etc.)?	A AWS fornece a capacidade para utilizar tags em recursos do EC2. As tags do EC2, uma forma de metadados, podem ser usadas para criar nomes acessíveis, aprimorar o recurso de pesquisa e melhorar a coordenação entre vários usuários. O Console de Gerenciamento da AWS também oferece suporte ao uso de tags.
	DSI-01.3	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.
	DSI-01.4	Vocês podem fornecer a localização física/geografia de armazenamento de dados de um grupo de usuários 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 servidores estarão localizados. A AWS não moverá o conteúdo de clientes das regiões selecionadas sem notificá-los, exceto se necessário para cumprir a legislação ou atender a solicitações de entidades governamentais. Neste momento, existem doze regiões: Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon), Oeste dos EUA (Norte da Califórnia), AWS GovCloud (EUA) (Oregon), UE (Irlanda), UE (Frankfurt), Ásia-Pacífico (Seul), Ásia-Pacífico (Cingapura), Ásia-Pacífico (Tóquio), Ásia-Pacífico (Sydney), Região da China (Pequim) e América do Sul (São Paulo).
	DSI-01.5	Vocês podem fornecer a localização física/geografia de armazenamento de dados de um grupo de usuários com antecedência?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	DSI-01.6	Vocês seguem algum padrão de identificação de dados estruturados (por exemplo, ISO 15489, Oasis XML Catalog Specification, diretriz de tipo de dados 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.
	DSI-01.7	Vocês permitem que grupos de usuários definam locais geográficos aceitáveis para roteamento de dados ou instanciação de recursos?	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 servidores estarão localizados. A AWS não moverá o conteúdo de clientes das regiões selecionadas sem notificá-los, exceto se necessário para cumprir a legislação ou atender a solicitações de entidades governamentais. Neste momento, existem doze regiões: Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon), Oeste dos EUA (Norte da Califórnia), AWS GovCloud (EUA) (Oregon), UE (Irlanda), UE (Frankfurt), Ásia-Pacífico (Seul), Ásia-Pacífico (Cingapura), Ásia-Pacífico (Tóquio), Ásia-Pacífico (Sydney), Região da China (Pequim) e América do Sul (São Paulo).
Segurança de dados e gerenciamento do ciclo de vida das informações *Inventário/ Fluxos de Dados*	DSI-02.1	Vocês armazenam, documentam e mantêm fluxos de dados que residem (permanente ou temporariamente) nas aplicações de serviços e nos sistemas e redes de infraestrutura?	Os clientes da AWS podem designar em qual região física seu conteúdo estará localizado. A AWS não moverá o conteúdo de clientes das regiões selecionadas sem notificá-los, exceto se necessário para cumprir a legislação ou atender a solicitações de entidades governamentais. Neste momento, existem doze regiões: Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon), Oeste dos EUA (Norte da Califórnia), AWS GovCloud (EUA) (Oregon), UE (Irlanda), UE (Frankfurt), Ásia-Pacífico (Seul), Ásia-Pacífico (Cingapura), Ásia-Pacífico (Tóquio), Ásia-Pacífico (Sydney), Região da China (Pequim) e América do Sul (São Paulo).
	DSI-02.2	Vocês podem garantir que os dados não serão migrados além de uma fronteira geográfica definida?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Segurança de dados e gerenciamento do ciclo de vida das informações *Transações de comércio eletrônico*	DSI-03.1	Vocês fornecem metodologias de criptografia aberta (3.4ES, AES, etc.) para grupos de usuários a fim de solicitar que eles protejam seus dados se for necessário trafegar por redes públicas (por exemplo, a Internet)?	Todas as APIs da AWS estão disponíveis através de endpoints protegidos por SSH 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. Os túneis IPSec para a VPC também são criptografados. Além disso, os clientes podem aproveitar o AWS Key Management Systems (KMS) para criar e controlar chaves de criptografia (consulte https://aws.amazon.com/kms/). Os clientes também podem usar tecnologias de criptografia de terceiros. Consulte o Whitepaper de Segurança na Nuvem AWS para obter detalhes adicionais, disponível em http://aws.amazon.com/security.
	DSI-03.2	Vocês utilizam metodologias de criptografia aberta sempre que seus componentes de infraestrutura precisam se comunicar utilizando redes públicas (por exemplo, replicação de dados via Internet de um ambiente para outro)?	
Segurança de dados e gerenciamento do ciclo de vida das informações *Política de segurança/ rotulamento/ identificação*	DSI-04.1	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 dos dados e podem implementar procedimentos e políticas de identificação e rotulagem, a fim de atender às exigências deles.
	DSI-04.2	Há mecanismos de herança de rótulo implementados para objetos que atuam como recipientes agregados para dados?	
Segurança de dados e gerenciamento do ciclo de vida das informações *Dados não relativos à produção*	DSI-05.1	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.

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Segurança de dados e gerenciamento do ciclo de vida das informações *Propriedade/ administração*	DSI-06.1	As responsabilidades relacionadas à administração de dados são definidas, atribuídas, documentadas e transmitidas?	Os clientes da AWS mantêm o controle e a propriedade sobre os seus próprios dados. Consulte o Contrato do Cliente da AWS para obter mais informações.
Segurança de dados e gerenciamento do ciclo de vida das informações *Descarte seguro*	DSI-07.1	Vocês oferecem suporte à exclusão segura (por exemplo, limpeza criptográfica/inutilização) de dados arquivados e com backup como determinado pelo grupo de usuários?	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 não for possível desativar um dispositivo de hardware usando esses procedimentos, o dispositivo será inutilizado ou fisicamente destruído em conformidade com as práticas padrão do setor. Consulte o Whitepaper de Segurança na Nuvem AWS para obter detalhes adicionais, disponível em http://aws.amazon.com/security. Os volumes do Amazon EBS são apresentados como dispositivos de blocos não formatados brutos, que foram limpos antes de serem disponibilizados para uso. A limpeza ocorre imediatamente antes da reutilização. Assim, você pode ter certeza de que o processo de limpeza foi concluído. Se você tiver procedimentos que exigem que todos os dados sejam eliminados através de um método específico, como os detalhados no DoD 5220.22-M ("Manual de operação do programa nacional de segurança industrial") ou NIST 800-88 ("Orientações para o tratamento de mídia"), poderá fazê-lo no Amazon EBS. Você deve realizar um procedimento especializado de limpeza antes de excluir o volume para a conformidade com as normas estabelecidas.

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	DSI-07.2	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?	A criptografia de dados confidenciais geralmente é uma boa prática de segurança. A AWS permite a criptografia de volumes do EBS e de seus snapshots com AES-256. A criptografia ocorre nos servidores que hospedam as instâncias do EC2, processando-se durante o trânsito dos dados entre as instâncias do EC2 e o armazenamento no EBS. Para poder fazer isso com eficiência e baixa latência, o recurso de criptografia do EBS só está disponível nos tipos mais potentes de instâncias do EC2 (ex.: M3, C3, R3 e G2).
Segurança do Datacenter *Gerenciamento de ativos*	DCS-01.1	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 suprimentos e aquisição da AWS mantém relações com todos os fornecedores da AWS. Consulte o padrão ISO 27001, Anexo A, domínio 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.
	DCS-01.2	Vocês mantêm um inventário completo de todas as suas relações com fornecedores essenciais?	
Segurança do Datacenter *Pontos de acesso controlado*	DCS-02.1	Há perímetros de segurança física (por exemplo, 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 de forma exclusiva, controles de perímetro como cerca, muros, equipe de segurança, vigilância com vídeo, sistemas de detecção de intrusão e outros meios eletrônicos. Os relatórios SOC da AWS fornecem mais detalhes sobre atividades específicas de controle executadas pela AWS. Consulte o padrão ISO 27001, Anexo A, domínio 11 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 do Datacenter *Identificação de equipamento*	DCS-03.1	A identificação de equipamento automatizada é usada como um método para 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.

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Segurança do Datacenter *Autorização fora do local*	DCS-04.1	Vocês fornecem a grupos de usuários 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 notificá-los, exceto se necessário para cumprir a legislação ou atender a solicitações de entidades governamentais. Consulte o Whitepaper de Segurança na Nuvem AWS para obter detalhes adicionais, disponível em http://aws.amazon.com/security.
Segurança do Datacenter *Equipamento fora do local*	DCS-05.1	Vocês fornecem aos grupos de clientes evidências que documentam 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 não for possível desativar um dispositivo de hardware 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, domínio 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.
Segurança do Datacenter *Política*	DCS-06.1	Vocês podem fornecer evidências de que foram estabelecidos procedimentos, padrões 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. Os relatórios SOC da AWS fornecem detalhes adicionais sobre atividades específicas de controle de segurança física executadas pela AWS. Consulte o padrão ISO 27001, Anexo A, domínio 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.

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	DCS-06.2	Vocês fornecem evidências de que sua equipe e terceiros envolvidos foram treinados nos procedimentos, padrões e políticas documentados?	Em alinhamento com o padrão ISO 27001, todos os funcionários da AWS realizam treinamento periódico em segurança da informação, o qual requer uma confirmação para sua conclusão. As auditorias de conformidade são realizadas periodicamente para validar que os funcionários entendem e seguem as políticas estabelecidas. Consulte o Whitepaper de Segurança na Nuvem AWS para obter detalhes adicionais, disponível em http://aws.amazon.com/security. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com a certificação ISO 27001. Além disso, os relatórios SOC 1 e SOC 2 da AWS fornecem informações adicionais.
Segurança do Datacenter *Autorização de área segura*	DCS-07.1	Vocês permitem que grupos de usuários especifiquem em quais de seus locais geográficos os dados deles 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 designam em qual região física seus dados estarão localizados. A AWS não moverá o conteúdo de clientes das regiões selecionadas sem notificá-los, exceto se necessário para cumprir a legislação ou atender a solicitações de entidades governamentais. Neste momento, existem doze regiões: Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon), Oeste dos EUA (Norte da Califórnia), AWS GovCloud (EUA) (Oregon), UE (Irlanda), UE (Frankfurt), Ásia-Pacífico (Seul), Ásia-Pacífico (Cingapura), Ásia-Pacífico (Tóquio), Ásia-Pacífico (Sydney), Região da China (Pequim) e América do Sul (São Paulo).
Segurança do Datacenter *Entrada de pessoas não autorizadas*	DCS-08.1	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 dos 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 pelo menos duas vezes por uma autenticação de dois fatores para ter acesso aos andares do datacenter. Os pontos de acesso físico aos locais de servidores são registrados por um circuito fechado de TV (CCTV), conforme definido na política de segurança física de datacenters da AWS.

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Segurança do Datacenter *Acesso do usuário*	DCS-09.1	Vocês restringem o acesso físico de usuários e da equipe de suporte a ativos de informação e funções?	Os mecanismos de segurança física da AWS são revisados por auditores externos independentes durante as nossas auditorias de conformidade com SOC, PCI DSS, ISO 27001 e FedRAMP.
Gerenciamento de chave e criptografia *Qualificação*	EKM-01.1	Vocês têm políticas de gerenciamento de chave que associam chaves a proprietários identificáveis?	A AWS permite que os clientes usem seus próprios mecanismos de criptografia para quase todos os serviços, incluindo S3, EBS e EC2. As sessões da VPC também são criptografadas. Além disso, os clientes podem aproveitar o AWS Key Management Systems (KMS) para criar e controlar chaves de criptografia (consulte https://aws.amazon.com/kms/). Internamente, a AWS estabelece e gerencia chaves criptográficas para a criptografia necessária empregada na infraestrutura da AWS. Um gerenciador de credenciais e chaves de segurança desenvolvido pela AWS é usado para criar, proteger e distribuir chaves simétricas, além de proteger e distribuir: credenciais da AWS necessárias em hosts, chaves públicas/privadas de RSA e Certificações X.509. Os processos criptográficos da AWS são revisados por auditores terceirizados independentes, como parte da conformidade contínua com SOC, PCI DSS, ISO 27001 e FedRAMP.
Gerenciamento de chave e criptografia *Criação de chaves*	EKM-02.1	Vocês têm recursos para permitir a criação de chaves de criptografia exclusivas por grupo de usuários?	A AWS permite que os clientes usem seus próprios mecanismos de criptografia para quase todos os serviços, incluindo S3, EBS e EC2. Os túneis IPSec para a VPC também são criptografados. Além disso, os clientes podem aproveitar o AWS Key Management Systems (KMS) para criar e controlar chaves de criptografia (consulte https://aws.amazon.com/kms/). Consulte os relatórios SOC da AWS para obter mais detalhes sobre o KMS. Além disso, consulte o Whitepaper de Segurança na Nuvem AWS para obter detalhes adicionais, disponível em http://aws.amazon.com/security.
	EKM-02.2	Vocês têm recursos para gerenciar chaves de criptografia em nome de grupos de usuários?	
	EKM-02.3	Vocês mantêm procedimentos de gerenciamento de chaves?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	EKM-02.4	Vocês têm propriedade documentada para cada estágio do ciclo de vida de chaves de criptografia?	Internamente, a AWS estabelece e gerencia chaves criptográficas para a criptografia necessária empregada na infraestrutura da AWS. A AWS produz, controla e distribui chaves criptográficas simétricas usando tecnologias e processos de gerenciamento de chaves comprovados no sistema de informações da AWS. Um gerenciador de credenciais e chaves de segurança desenvolvido pela AWS é usado para criar, proteger e distribuir chaves simétricas, além de proteger e distribuir: credenciais da AWS necessárias em hosts, chaves públicas/ privadas de RSA e Certificações X.509. Os processos criptográficos da AWS são revisados por auditores terceirizados independentes, como parte da conformidade contínua com SOC, PCI DSS, ISO 27001 e FedRAMP.
	EKM-02.5	Vocês utilizam alguma estrutura de terceiros/de código aberto/própria para gerenciar chaves de criptografia?	
Gerenciamento de chave e criptografia *Criptografia*	EKM-03.1	Vocês criptografam dados de grupos de clientes 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 e EC2. Os túneis IPSec para a VPC também são criptografados. Além disso, os clientes podem aproveitar o AWS Key Management Systems (KMS) para criar e controlar chaves de criptografia (consulte https://aws.amazon.com/kms/). Consulte os relatórios SOC da AWS para obter mais detalhes sobre o KMS. Além disso, consulte o Whitepaper de Segurança na Nuvem AWS para obter detalhes adicionais, disponível em http://aws.amazon.com/security.
	EKM-03.2	Vocês utilizam criptografia para proteger imagens de máquina virtual e dados durante o transporte em e entre instâncias de hypervisor e redes?	
	EKM-03.3	Vocês oferecem suporte a chaves de criptografia geradas por grupo de usuários ou permitem que esses grupos criptografem dados em uma identidade, sem acesso a um certificado de chave pública (por exemplo, criptografia com base em identidade)?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	EKM-03.4	Vocês têm alguma documentação que estabelece e define procedimentos, diretrizes e políticas de gerenciamento de criptografia?	
Gerenciamento de chave e criptografia *Armazenamento e acesso*	EKM-04.1	Vocês têm plataforma e criptografia de dados apropriada que usa formatos abertos/ validados e algoritmos padrão?	A AWS permite que os clientes usem seus próprios mecanismos de criptografia para quase todos os serviços, incluindo S3, EBS e EC2. Além disso, os clientes podem aproveitar o AWS Key Management Systems (KMS) para criar e controlar chaves de criptografia (consulte https://aws.amazon.com/kms/). Consulte os relatórios SOC da AWS para obter mais detalhes sobre o KMS. A AWS estabelece e gerencia chaves criptográficas para a criptografia necessária empregada na infraestrutura da AWS. A AWS produz, controla e distribui chaves criptográficas simétricas usando tecnologias e processos de gerenciamento de chaves comprovados no sistema de informações da AWS. Um gerenciador de credenciais e chaves de segurança desenvolvido pela AWS é usado para criar, proteger e distribuir chaves simétricas, além de proteger e distribuir: credenciais da AWS necessárias em hosts, chaves públicas/privadas de RSA e Certificações X.509. Os processos criptográficos da AWS são revisados por auditores terceirizados independentes, como parte da conformidade contínua com SOC, PCI DSS, ISO 27001 e FedRAMP.
	EKM-04.2	Suas chaves de criptografia são mantidas pelo cliente da nuvem ou por um fornecedor confiável de gerenciamento de chave?	
	EKM-04.3	Vocês armazenam chaves de criptografia na nuvem?	
	EKM-04.4	Vocês têm funções separadas de gerenciamento e uso de chave?	
Governança e Gerenciamento de Risco *Requisitos da linha de base*	GRM-01.1	Vocês têm linhas de base de segurança da informação documentadas para cada componente de sua infraestrutura (por exemplo, hypervisor, 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 14 e 18 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. 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.

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	GRM-01.2	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?	
	GRM-01.3	Vocês permitem que clientes forneçam sua própria imagem de máquina virtual confiável, a fim de garantir a conformidade com seus próprios padrões internos?	
Governança e Gerenciamento de Risco *Avaliações de riscos*	GRM-02.1	Vocês fornecem dados de saúde de controle de segurança, a fim de permitir que grupos de usuários implementem monitoramento contínuo padrão do setor (que permite a validação contínua de grupos de usuários 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.
	GRM-02.2	Vocês realizam avaliações de risco associadas aos requisitos de governança de dados pelo menos uma vez por ano?	Em alinhamento com a norma ISO 27001, a AWS mantém um programa de gerenciamento de riscos para minimizar e gerenciar riscos. Além disso, a AWS mantém uma certificação AWS ISO 27018. A conformidade com o ISO 27018 demonstra para os clientes que a AWS tem um sistema de controles em vigor que aborda especificamente a proteção de privacidade do conteúdo. Para obter mais informações, consulte as perguntas frequentes sobre a conformidade da AWS com ISO 27018 http://aws.amazon.com/compliance/iso-27018-faqs/.

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Governança e Gerenciamento de Risco *Supervisão de gerenciamento*	GRM-03.1	Seus gerentes técnicos, comerciais e executivos são responsáveis por manter a familiarização e o cumprimento de políticas, procedimentos e padrões de segurança para si mesmos e seus funcionários, visto que pertencem à área de responsabilidade do gerente e dos funcionários?	O ambiente de controle na Amazon começa no mais alto nível da Empresa. As lideranças executiva e sênior desempenham um papel importante no estabelecimento de valores fundamentais e do objetivo da empresa. Cada funcionário recebe o código de conduta e ética nos negócios da empresa, além de realizar 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 mais detalhes. Disponível em http://aws.amazon.com/compliance.
Governança e Gerenciamento de Risco *Programa de gerenciamento*	GRM-04.1	Vocês fornecem a grupos de usuários documentação descrevendo seu ISMP (Information Security Management Program, Programa de gerenciamento de segurança da informação)?	A AWS fornece aos clientes nossa certificação ISO 27001. A certificação ISO 27001 é voltada especificamente para o AWS ISMS e avalia como os processos internos da AWS seguem o padrão ISO. A certificação indica que um auditor independente reconhecido por terceiros avaliou nossos processos e controles e confirma que eles estão operando de acordo com o padrão de certificação ISO 27001. Para obter mais informações, consulte o site de perguntas frequentes sobre a conformidade da AWS com ISO 27001: http://aws.amazon.com/compliance/iso-27001-faqs/.
	GRM-04.2	Vocês analisam seu programa de gerenciamento de segurança de informações (ISMP) pelo menos uma vez por ano?	
Governança e Gerenciamento de Risco *Envolvimento/ suporte de gerenciamento*	GRM-05.1	Vocês garantem que seus provedores seguem suas políticas de privacidade e segurança da informação?	A AWS estabeleceu políticas e uma estrutura de segurança da informação que integraram com eficácia a estrutura certificável por ISO 27001, com base em controles do ISO 27002, nos princípios de serviços de confiança do AICPA (American Institute of Certified Public Accountants), na PCI DSS v3.1 e na Publicação 800-53 do NIST (National Institute of Standards and Technology) sobre controles de segurança recomendados para sistemas de informação federais. A AWS gerencia relações de terceiros de acordo com os padrões ISO 27001.
Governança e Gerenciamento de Risco *Política*	GRM-06.1	Suas políticas de privacidade e segurança da informação estão alinhadas a padrões do setor (ISO-27001, ISO-22307, CoBIT etc.)?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	GRM-06.2	Vocês têm contratos que garantem que seus provedores seguem suas políticas de privacidade e segurança da informação?	Os requisitos de terceiros da AWS são revisados por auditores externos independentes durante as nossas auditorias de conformidade com PCI DSS, ISO 27001 e FedRAMP. Informações sobre os programas de conformidade da AWS são publicadas e disponibilizadas em nosso site em http://aws.amazon.com/compliance/.
	GRM-06.3	Vocês podem fornecer evidências de mapeamento de auditoria detalhada de seus controles, arquitetura e processos para regulamentos e/ou padrões?	
	GRM-06.4	Vocês divulgam com quais controles, padrões, certificações e/ou normas estão em conformidade?	
Governança e Gerenciamento de Risco *Aplicação de política*	GRM-07.1	Há uma política de sanção ou disciplinar formal estabelecida para funcionários que violaram procedimentos e políticas de segurança?	A AWS fornece políticas de segurança e treinamento em segurança para funcionários, a fim de instruí-los em sua função e responsabilidades relativas à segurança da informação. Os funcionários que violarem protocolos ou padrões da Amazon serão investigados e submetidos à ação disciplinar apropriada (p. ex., advertência, plano de desempenho, suspensão e/ou rescisão). Consulte o Whitepaper de Segurança na Nuvem AWS para obter detalhes adicionais, disponível em http://aws.amazon.com/security. Consulte o padrão ISO 27001, Anexo A, domínio 7 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.
	GRM-07.2	Os funcionários estão cientes de quais ações podem ser tomadas em caso de violação de políticas e procedimentos?	
Governança e Gerenciamento de Risco *Impactos de alterações de política/ negócios*	GRM-08.1	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 para obter mais informações. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com a certificação ISO 27001.

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Governança e Gerenciamento de Risco *Revisões de política*	GRM-09.1	Vocês notificam seus grupos de usuários quando fazem alterações materiais em suas políticas de privacidade e/ou segurança da informação?	Os Whitepapers sobre Segurança da Nuvem AWS e Risco e Conformidade, disponíveis em http://aws.amazon.com/security e http://aws.amazon.com/compliance, são atualizados regularmente para refletir as modificações em políticas da AWS.
	GRM-09.2	Vocês realizam análises no mínimo manuais nas políticas de privacidade e segurança?	Os relatórios SOC da AWS fornecem detalhes relacionados à análise da política de privacidade e segurança.
Governança e Gerenciamento de Risco *Avaliações*	GRM-10.1	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 a 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.
	GRM-10.2	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)?	
Governança e Gerenciamento de Risco *Programa*	GRM-11.1	Vocês têm um programa documentado em toda a organização em vigor para gerenciar riscos?	Em alinhamento com ISO 27001, a AWS mantém um programa de gerenciamento de riscos para minimizar e gerenciar riscos. A gerência da AWS tem 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 que o gerenciamento identifique riscos em suas áreas de

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	GRM-11.2	Vocês disponibilizam a documentação do programa de gerenciamento de risco de toda a organização?	responsabilidade, bem como implemente medidas adequadas projetadas para solucionar esses riscos. O programa de gerenciamento de riscos da AWS é revisado por auditores externos independentes durante as nossas auditorias de conformidade com PCI DSS, ISO 27001 e FedRAMP.
Recursos Humanos *Devoluções de ativos*	HRS-01.1	Há sistemas vigentes para monitorar violações de privacidade e notificar os grupos de usuários 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. Os relatórios SOC da AWS fornecem uma visão geral dos controles vigentes para monitorar o ambiente gerenciado da AWS.
	HRS-01.2	Sua política de privacidade está alinhada com os padrões do setor?	
Recursos Humanos *Triagem de histórico*	HRS-02.1	De acordo com as restrições contratuais, ética, regulamentos e legislações locais, todos os candidatos à contratação, contratantes e terceiros envolvidos 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. Os relatórios SOC da AWS fornecem detalhes adicionais relacionados aos controles vigentes para a verificação de antecedentes.
Recursos Humanos *Contratos empregatícios*	HRS-03.1	Vocês treinam especificamente seus funcionários em relação à sua função específica e aos controles de segurança de informações que eles devem seguir?	Em alinhamento com o padrão ISO 27001, todos os funcionários da AWS realizam treinamento periódico de acordo com a função, que inclui treinamento em segurança da AWS e requer uma confirmação para sua conclusão. As auditorias de conformidade são realizadas periodicamente para validar que os funcionários entendem e seguem as políticas estabelecidas. Consulte os relatórios SOC para obter mais detalhes. Toda a equipe que oferece suporte aos sistemas e dispositivos da AWS deve assinar um acordo de confidencialidade antes de receber acesso. Além disso, após a contratação, a equipe deve ler e aceitar a Política de Uso Aceitável e a Política de Código de Ética e Conduta nos negócios da Amazon (Código de conduta).
	HRS-03.2	Vocês documentam a confirmação do treinamento que o funcionário concluiu?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	HRS-03.3	Toda a equipe é obrigada a assinar um NDA ou Contratos de Confidencialidade como condição de contratação para proteger as informações do cliente/ grupo de usuários?	
	HRS-03.4	A conclusão bem-sucedida e dentro do prazo do programa de treinamento é considerada um pré-requisito para adquirir e manter o acesso a sistemas confidenciais?	
	HRS-03.5	A equipe é treinada e passa por programas de familiarização pelo menos uma vez por ano?	
Recursos Humanos *Término de contratação*	HRS-04.1	Existem políticas, diretrizes e procedimentos documentados em vigor para regular alterações em contratação e/ou término?	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. Os relatórios SOC da AWS fornecem detalhes adicionais.
	HRS-04.2	Os procedimentos e diretrizes acima são responsáveis pela revogação de acesso e pela devolução de bens apropriadas?	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. Os relatórios SOC da AWS fornecem 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, domínio 7 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.

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Recursos Humanos *Dispositivos móveis/ portáteis*	HRS-05.1	Há políticas e procedimentos estabelecidos e medidas implementadas para limitar rigidamente o acesso a seus dados confidenciais e a dados do grupo de usuários a partir de dispositivos móveis e portáteis, como laptops, celulares e PDAs, que geralmente apresentam risco maior do que dispositivos não portáteis (p. ex., computadores desktop nas instalações da organização do provedor)?	Os clientes mantêm o controle e a responsabilidade sobre os seus dados e ativos de mídia associados. O cliente é responsável por gerenciar dispositivos móveis de segurança e o acesso à autorização do cliente.
Recursos Humanos *Acordos de confiden-cialidade*	HRS-06.1	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.
Recursos Humanos *Funções/ responsa-bilidades*	HRS-07.1	Vocês fornecem a grupos de usuários um documento de definição de função esclarecendo suas responsabilidades administrativas versus as do grupo de usuários?	Os Whitepapers de Segurança da Nuvem AWS e de Conformidade e Risco 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/security e http://aws.amazon.com/compliance.
Recursos Humanos *Uso aceitável*	HRS-08.1	Vocês fornecem documentação em relação a como podem vir a utilizar ou acessar metadados e dados de locatários?	A AWS possui uma política de controle de acesso formal que é revisada e atualizada anualmente (ou quando ocorre uma alteração importante no sistema que afeta a política). A política aborda o propósito, o escopo, as funções, as responsabilidades e o compromisso com o gerenciamento. A AWS emprega o conceito de menor privilégio, permitindo somente o acesso necessário para que os usuários executem suas funções de trabalho.

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	HRS-08.2	Vocês coletam ou criam metadados sobre uso de dados de grupos de usuários por meio de tecnologias de inspeção (mecanismos de pesquisa etc.)?	Os clientes mantêm o controle e a responsabilidade sobre os seus dados e ativos de mídia associados. O cliente é responsável por gerenciar dispositivos móveis de segurança e o acesso à autorização do cliente. Consulte o padrão ISO 27001 e o código de prática 27018 para obter mais informações. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com os padrões ISO 27001 e ISO 27018.
	HRS-08.3	Vocês permitem que grupos de usuários neguem o acesso aos dados/metadados deles por meio de tecnologias de inspeção?	
Recursos Humanos *Treinamento/ Familiarização*	HRS-09.1	Vocês fornecem um programa de treinamento formal e baseado em função sobre conhecimento de segurança para questões de gerenciamento de dados e acesso relacionado à nuvem (por exemplo, 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 uma confirmação para sua conclusão. As auditorias de conformidade são realizadas periodicamente para validar que os funcionários entendem e seguem as políticas estabelecidas. As funções e responsabilidades da AWS são revisadas por auditores externos independentes durante as nossas auditorias de conformidade com SOC, PCI DSS, ISO 27001 e FedRAMP.
	HRS-09.2	Os administradores de dados e gerentes são devidamente instruídos sobre suas responsabi-lidades legais em relação à segurança e à integridade de dados?	
Recursos Humanos *Responsa-bilidade do usuário*	HRS-10.1	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 compreender suas responsabilidades e funções individuais e a comunicar 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

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	HRS-10.2	Os usuários estão cientes de suas responsabilidades por manter um ambiente de trabalho seguro e protegido?	intranet da Amazon. Consulte o padrão ISO 27001, Anexo A, domínios 7 e 8. 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 Segurança na Nuvem AWS fornece mais detalhes, disponível em http://aws.amazon.com/security.
	HRS-10.3	Os usuários estão cientes de suas responsabilidades por deixar equipamentos não assistidos de forma segura?	
Recursos Humanos *Área de trabalho*	HRS-11.1	Seus procedimentos e políticas de gerenciamento de dados solucionam os conflitos de interesses em nível de serviço e grupo de usuários?	As políticas de gerenciamento de dados da AWS estão alinhadas com o padrão ISO 27001. Consulte o padrão ISO 27001, Anexo A, domínios 8 e 9. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001. Os relatórios SOC da AWS fornecem detalhes adicionais sobre atividades específicas de controle executadas pela AWS para impedir o acesso não autorizado aos recursos desta. A AWS identificou categorias de eventos auditáveis em sistemas e dispositivos da AWS. As equipes de serviço configuram os recursos de auditoria para registrar continuamente os eventos relacionados à segurança de acordo com os requisitos. Os registros de auditoria contêm um conjunto de elementos de dados para oferecer suporte aos requisitos de análise necessários. Além disso, os registros de auditoria estão disponíveis para que a equipe de segurança da AWS ou outras equipes responsáveis realizem inspeção ou análise sob demanda e em resposta a eventos relacionados à segurança ou de impacto comercial.
	HRS-11.2	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 grupo de usuários?	
	HRS-11.3	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?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Identity & Access Management *Acesso a ferramentas de auditoria*	IAM-01.1	Vocês restringem, registram e monitoram o acesso aos seus sistemas de gerenciamento de segurança da informação (por exemplo, hypervisor, 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. Os relatórios SOC da AWS descrevem os controles vigentes para gerenciar o provisionamento a recursos da AWS. Consulte o Whitepaper de Segurança na Nuvem AWS para obter detalhes adicionais, disponível em http://aws.amazon.com/security.
	IAM-01.2	Vocês monitoram e registram acesso privilegiado (nível de administrador) a sistemas de gerenciamento de segurança de informações?	A AWS identificou categorias de eventos auditáveis em sistemas e dispositivos da AWS. As equipes de serviço configuram os recursos de auditoria para registrar continuamente os eventos relacionados à segurança de acordo com os requisitos. O sistema de armazenamento de logs foi projetado para fornecer um serviço altamente escalonável e disponível que aumenta a capacidade de acordo com a necessidade de crescimento do armazenamento de logs. Os registros de auditoria contêm um conjunto de elementos de dados para oferecer suporte aos requisitos de análise necessários. Além disso, os registros de auditoria estão disponíveis para que a equipe de segurança da AWS ou outras equipes responsáveis realizem inspeção ou análise sob demanda e em resposta a eventos relacionados à segurança ou de impacto comercial. A equipe designada nas equipes da AWS recebe alertas automatizados no caso de falha de processamento de auditoria. As falhas de processamento de auditoria incluem, por exemplo, erros de software/hardware. Quando alertada, a equipe de plantão emite uma identificação do problema e acompanha o evento até que ele seja resolvido. Os processos de log e monitoramento da AWS são revisados por auditores terceirizados independentes, como parte da conformidade contínua com o SOC, PCI DSS, ISO 27001 e FedRAMP.

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Identity & Access Management *Política de acesso de usuário*	IAM-02.1	Vocês têm controles vigentes para garantir a remoção em tempo hábil de acessos ao sistema que não sejam mais necessários para fins comerciais?	Os relatórios SOC da AWS fornecem 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, domínio 9 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.
	IAM-02.2	Vocês fornecem métricas que controlam com que rapidez é possível remover o acesso a sistemas que não seja mais necessário para fins comerciais?	
Identity & Access Management *Acesso a portas de configuração/ diagnóstico*	IAM-03.1	Vocês usam redes seguras dedicadas para fornecer acesso de gerenciamento à sua infraestrutura de serviço em nuvem?	Os controles implementados limitam o acesso aos sistemas e aos dados, fornecendo acesso restrito e monitorado de acordo com a política de acesso da AWS. Além disso, por padrão, os dados do cliente e as instâncias do servidor são logicamente isolados de outros clientes. Os controles de acesso de usuário privilegiado são revistos por um auditor independente durante as auditorias SOC da AWS, ISO 27001, PCI, ITAR e da FedRAMP.
Identity & Access Management *Políticas e procedimentos*	IAM-04.1	Vocês gerenciam e armazenam a identidade de toda a equipe que tem acesso à infraestrutura de TI, incluindo o nível de acesso?	
	IAM-04.2	Vocês gerenciam e armazenam a identidade de usuário de toda a equipe que tem acesso à rede, incluindo o nível de acesso?	
Identity & Access Management *Segregação de tarefas*	IAM-05.1	Vocês fornecem aos grupos de usuários 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 está alinhada ao padrão ISO 27001 para gerenciamento de segregação de tarefas. Consulte o padrão ISO 27001, Anexo A, domínio 6 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.

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Identity & Access Management *Restrição de acesso a código fonte*	IAM-06.1	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 os padrões ISO 27001, a AWS estabeleceu procedimentos e políticas formais para delinear os padrões mínimos para acesso lógico a recursos da AWS. Os relatórios SOC da AWS descrevem 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 mais detalhes, disponível em http://aws.amazon.com/security.
	IAM-06.2	Há controles vigentes para impedir o acesso não autorizado ao código-fonte de aplicações, programas ou objetos do grupo de usuários e garantir que ele esteja restrito somente à equipe autorizada?	
Identity & Access Management *Acesso de terceiros*	IAM-07.1	Vocês fornecem capacidade de recuperação de desastres no caso de várias falhas?	A AWS oferece aos clientes a flexibilidade de posicionar 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 os relatórios SOC da AWS. O padrão ISO 27001, Anexo A, domínio 15 oferece mais detalhes. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com a certificação ISO 27001.
	IAM-07.2	Vocês monitoram a continuidade de serviço com provedores upstream na hipótese de falha do provedor?	
	IAM-07.3	Vocês têm mais de um provedor para cada serviço com o qual contam?	
	IAM-07.4	Vocês fornecem acesso a resumos de continuidade e redundância operacional, incluindo os serviços com os quais contam?	
	IAM-07.5	Vocês fornecem ao grupo de usuários a capacidade de declarar um desastre?	
	IAM-07.6	Vocês fornecem ao grupo de usuários uma opção de failover acionado?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	IAM-07.7	Vocês compartilham seus planos de redundância e continuidade de negócios com seus grupos de usuários?	
Identity & Access Management *Autorização/ restrição de acesso de usuário*	IAM-08.1	Vocês documentam como concedem e aprovam o acesso a dados de grupos de usuários?	Os clientes da AWS mantêm o controle e a propriedade sobre os seus dados. Os controles implementados limitam o acesso a sistemas e dados, fornecendo acesso restrito e monitorado. Além disso, por padrão, os dados do cliente e as instâncias do servidor são logicamente isolados de outros clientes. Os controles de acesso de usuário privilegiado são revistos por um auditor independente durante as auditorias SOC da AWS, ISO 27001, PCI, ITAR e da FedRAMP.
	IAM-08.2	Vocês têm um método de alinhamento das metodologias de classificação de dados de grupos de usuários e provedor para fins de controle de acesso?	
Identity & Access Management *Autorização de acesso de usuário*	IAM-09.1	Sua equipe de gerenciamento fornece a autorização e restrições de acesso do usuário (por exemplo, funcionários, contratantes, clientes (grupos), parceiros de negócios e/ou fornecedores) antes que acessem os dados e quaisquer aplicações, sistemas de infraestrutura e componentes de rede próprios ou gerenciados (físicos e virtuais)?	Identificadores exclusivos de usuários são criados como parte do processo de fluxo de trabalho a bordo no sistema de gerenciamento de recursos humanos da AWS. O processo de provisionamento de dispositivos ajuda a garantir identificadores exclusivos para dispositivos. Ambos os processos incluem aprovação do gerente para estabelecer a conta ou o dispositivo do usuário. Os autenticadores iniciais são fornecidos ao usuário pessoalmente e para os dispositivos como parte do processo de provisionamento. Os usuários internos podem associar chaves públicas de SSH com suas contas. Os autenticadores de contas do sistema são fornecidos para o solicitante como parte do processo de criação de conta, após a verificação da identidade do solicitante.

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	IAM-09.2	Vocês fornecem, mediante solicitação, acesso do usuário (por exemplo, funcionários, contratantes, clientes (grupos), parceiros de negócios e/ou fornecedores) aos dados e quaisquer aplicações, sistemas de infraestrutura e componentes de rede próprios ou gerenciados (físicos e virtuais)?	A AWS estabeleceu controles para abordar a ameaça de acesso privilegiado inadequado. 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.
Identity & Access Management *Revisões de acesso de usuário*	IAM-10.1	Vocês exigem, pelo menos, uma certificação anual de qualificações de todos os administradores e usuários do sistema (exceto usuários mantidos por seus grupos de usuários)?	Em alinhamento com o padrão ISO 27001, todas as concessões de acesso são revisadas periodicamente; a reaprovação explícita é necessária ou o acesso ao recurso será automaticamente revogado. Os controles específicos para revisões de acesso de usuário são descritos nos relatórios SOC. As exceções nos controles de qualificação de usuário são documentadas nos relatórios SOC. Consulte os padrões ISO 27001, Anexo A, domínio 9 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.
	IAM-10.2	Se for detectado que os usuários não têm as qualificações necessárias, todas as ações de atualização e certificação serão registradas?	
	IAM-10.3	Vocês compartilham relatórios de atualização e certificação de qualificação de usuários com seus grupos no caso de acesso não adequado ter sido permitido a dados de grupos de usuários?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Identity & Access Management *Revogação de acesso de usuário*	IAM-11.1	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 envolvidos?	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. Os relatórios SOC da AWS fornecem 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, domínio 9 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.
	IAM-11.2	Alterações no status de acesso do usuário incluem término de contratação, contrato ou acordo, alteração de contratação ou transferência na organização?	
Identity & Access Management *Credenciais de ID de usuário*	IAM-12.1	Vocês oferecem suporte 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 identidades 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. O serviço AWS Identity and Access Management (IAM) oferece suporte à federação de identidades para acesso delegado ao Console de Gerenciamento da AWS ou a APIs da AWS. Com a federação de identidades, identidades externas (usuários federados) recebem acesso seguro aos recursos na conta da AWS sem precisar criar usuários do IAM. Essas identidades externas podem ser provenientes do seu provedor de identidades corporativas (como Microsoft Active Directory ou do AWS Directory Service) ou de um provedor de identidades da Web, como Amazon Cognito, Login with Amazon, Facebook, Google ou qualquer provedor compatível com OpenID Connect (OIDC).
	IAM-12.2	Vocês usam padrões abertos para delegar recursos de autenticação aos seus grupos de usuários?	
	IAM-12.3	Vocês oferecem suporte a padrões de federação de identidades (SAML, SPML, Federação WS etc.) como uma forma de autenticar/autorizar usuários?	
	IAM-12.4	Vocês têm algum recurso de ponto de imposição de política (por exemplo, XACML) para impor restrições jurídicas regionais e de política para o acesso do usuário?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	IAM-12.5	Vocês têm um sistema de gerenciamento de identidade vigente (que permite a classificação de dados para um grupo de usuários) para qualificação com base em contexto e funções para dados?	
	IAM-12.6	Vocês fornecem aos grupos de usuários opções rígidas de autenticação (multifator) (certificados digitais, tokens, biométrica etc.) para acesso de usuário?	
	IAM-12.7	Vocês permitem que os grupos de usuários utilizem serviços de garantia de identidade de terceiros?	
	IAM-12.8	Vocês oferecem suporte para política de senha (comprimento mínimo, idade, histórico, complexidade) e bloqueio de conta (limite de bloqueio, duração do bloqueio)?	O AWS Identity and Access Management (IAM) permite que você controle com segurança o acesso aos serviços e aos recursos da AWS para seus usuários. Informações adicionais sobre o IAM estão disponíveis no site em https://aws.amazon.com/iam/. Os relatórios SOC da AWS fornecem detalhes sobre atividades específicas de controle executadas pela AWS.
	IAM-12.9	Vocês permitem que grupos de usuários/ clientes definam políticas de senha e bloqueio da conta para suas contas?	
	IAM-12.10	Vocês oferecem algum recurso para forçar alterações de senha depois do primeiro login?	
	IAM-12.11	Vocês têm mecanismos vigentes para desblo-quear contas que foram bloqueadas (por exemplo, autoatendimento por e-mail, perguntas de desafio definidas, desbloqueio manual)?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Identity & Access Management *Acesso a programas de utilitários*	IAM-13.1	Há utilitários que podem gerenciar significativa-mente 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. Os relatórios SOC da AWS fornecem detalhes sobre atividades específicas de controle executadas pela AWS. Consulte o Whitepaper de Visão Geral de Processos de Segurança da AWS para obter mais detalhes, disponível em http://aws.amazon.com/security.
	IAM-13.2	Vocês têm recursos para detectar ataques que almejam a infraestrutura virtual diretamente (p. ex., “shimming”, “Blue Pill”, “Hyper jumping” etc.)?	
	IAM-13.3	Há ataques que almejam a infraestrutura virtual que sejam impedidos com controles técnicos?	
Infraestrutura e segurança de virtualização *Detecção de intrusão/ registro em log de auditoria*	IVS-01.1	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 padrões ISO 27001. Os utilitários do sistema são devidamente restritos e monitorados. Os relatórios SOC da AWS fornecem 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 mais detalhes, disponível em http://aws.amazon.com/security.
	IVS-01.2	Há acesso de usuário lógico e físico para auditar logs restritos à equipe autorizada?	
	IVS-01.3	Vocês podem fornecer evidências de que o mapeamento de auditoria detalhada de regula-mentos e padrões em seus controles/arquitetura/ processos foi feito?	
	IVS-01.4	Há logs de auditoria armazenados e retidos centralmente?	Em alinhamento com os padrões 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.

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	IVS-01.5	Os logs de auditoria são revisados regularmente quanto a eventos de segurança (por exemplo, com ferramentas automáticas)?	A AWS utiliza sistemas de monitoramento automatizados para fornecer um alto nível de disponibilidade e desempenho do serviço. O monitoramento proativo está disponível através de uma variedade de ferramentas on-line para uso interno e externo. Os sistemas dentro da AWS são extensivamente instrumentados para monitorar as principais métricas operacionais. Os alarmes são configurados para notificar operações e gerenciar colaboradores quando limites de alerta de início são cruzados nas principais métricas operacionais. Uma agenda de plantão é usada para que colaboradores estejam sempre disponíveis para auxiliar com problemas operacionais. Isso inclui um sistema de pager para que os alertas sejam comunicados de maneira rápida e confiável à equipe de operações. Consulte o Whitepaper de Segurança na Nuvem AWS para obter detalhes adicionais, disponível em http://aws.amazon.com/security.
Infraestrutura e segurança de virtualização *Detecção de alteração*	IVS-02.1	Vocês registram e enviam alertas sobre alterações feitas em imagens de máquina virtual independente-mente do estado de execução (por exemplo, pausada, desligada ou em execução)?	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.
	IVS-02.2	As alterações feitas em máquinas virtuais ou a mudança de uma imagem e a validação subsequente da integridade da imagem são disponibilizadas imediatamente para os clientes por meio de métodos eletrônicos (por exemplo, portais ou alertas)?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Infraestrutura e segurança de virtualização *Sincronização de relógio*	IVS-03.1	Vocês usam um protocolo de serviço de hora sincronizado (por exemplo, NTP) para garantir que todos os sistemas tenham uma referência de hora comum?	Em alinhamento com os padrões 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.
Infraestrutura e segurança de virtualização *Planejamento de recursos/ capacidade*	IVS-04.1	Vocês fornecem documentação em relação a quais níveis de assinatura em excesso do sistema (rede, armazenamento, memória, E/S etc.) e em quais circunstâncias/ cenários?	Detalhes sobre limites de serviço da AWS e como solicitar um aumento para serviços específicos estão disponíveis no site da AWS em http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html. 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.
	IVS-04.2	Vocês restringem o uso das capacidades de assinatura em excesso de memória presentes no hypervisor?	
	IVS-04.3	Seus requisitos de capacidade do sistema levam em conta necessidades de capacidade atuais, projetadas e previstas para todos os sistemas usados para fornecer serviços aos grupos de usuários?	
	IVS-04.4	O desempenho do sistema é monitorado e ajustado para satisfazer constantemente requisitos normativos, contratuais e comerciais para todos os sistemas usados para fornecer serviços aos grupos de usuários?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Infraestrutura e segurança de virtualização *Gerenciamento – gerencia-mento de vulnerabilidades*	IVS-05.1	As ferramentas ou os serviços de avaliação de vulnerabilidade de segurança acomodam as tecnologias de virtualização usadas (por exemplo, reconhecimento de virtualização)?	O Amazon EC2 atualmente utiliza uma versão altamente personalizada do hypervisor Xen. O hypervisor é regularmente avaliado para verificar vulnerabilidades novas e existentes e vetores de ataque por equipes de penetração interna e externa e é bem adequado para manter um rígido isolamento entre máquinas virtuais convidadas. O hypervisor AWS Xen é regularmente avaliado por auditores independentes durante avaliações e auditorias. As varreduras de vulnerabilidade regulares internas e externas são realizadas no sistema operacional de host, na aplicação web e nos bancos de dados do ambiente da AWS através de várias ferramentas. A varredura de vulnerabilidade e as práticas de remediação são revisadas regularmente como parte da conformidade contínua da AWS com o PCI DSS e o FedRAMP.
Infraestrutura e segurança de virtualização *Segurança de rede*	IVS-06.1	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 da AWS fornece orientações sobre como criar uma arquitetura de segurança em camadas em vários whitepapers, disponíveis no site público da AWS – http://aws.amazon.com/documentation/.
	IVS-06.2	Vocês atualizam regularmente diagramas de arquitetura de rede que incluem fluxos de dados entre domínios/ zonas de segurança?	Dispositivos de proteção de perímetro que utilizam conjuntos de regras, Access Control Lists (ACL - Listas de controle de acesso) e configurações reforçam o fluxo de informações entre estruturas de rede. Existem várias estruturas de rede na Amazon, cada uma separada por dispositivos que controlam o fluxo de informações entre si. O fluxo de informações entre estruturas é estabelecido por autorizações aprovadas, que existem como Access Control Lists (ACL - Listas de controle de acesso) dentro desses dispositivos. Esses dispositivos controlam o fluxo de informações entre as estruturas, conforme exigido por essas ACLs. As ACLs são definidas, aprovadas pela equipe responsável, gerenciadas e implantadas usando a ferramenta de gerenciamento da AWS.
	IVS-06.3	Vocês revisam regularmente a adequação da conectividade/acesso permitido (por exemplo, regras de firewall) entre domínios/zonas de segurança na rede?	
	IVS-06.4	Todas as listas de controle de acesso do firewall são documentadas com justificativa de negócios?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Infraestrutura e segurança de virtualização *Proteção e Controles Base do SO*	IVS-07.1	Os sistemas operacionais são protegidos para fornecer somente as portas, os protocolos e serviços necessários para satisfazer as necessidades de negócios usando controles técnicos (isto é, monitoramento e registro de integridade do arquivo) como parte do padrão ou modelo básico de criação?	A equipe de segurança da informação da Amazon aprova essas ACLs. Os conjuntos de regras de firewall e as listas de controle de acesso aprovadas entre as estruturas de rede restringem o fluxo de informações para serviços de sistemas de informações específicos. As listas de controle de acesso e os conjuntos de regras são revisados, aprovados e automaticamente enviados para dispositivos de proteção do perímetro periodicamente (pelo menos a cada 24 horas) para garantir que os conjuntos de regras e as listas de controle de acesso estão atualizadas. O gerenciamento de rede da AWS é revisado regularmente por auditores terceirizados independentes, como parte da conformidade contínua da AWS com SOC, PCI DSS, ISO 27001 e FedRAMPsm. A AWS implementa o mínimo de privilégios possível em todos os componentes da sua infraestrutura. A AWS proíbe todas as portas e protocolos que não tenham uma finalidade comercial específica. A AWS segue uma abordagem rigorosa para implementação mínima dos recursos e funções que são essenciais para o uso do dispositivo. A varredura de rede é executada, e quaisquer portas ou protocolos desnecessários que estiverem em uso são corrigidos. As varreduras de vulnerabilidade regulares internas e externas são realizadas no sistema operacional de host, na aplicação web e nos bancos de dados do ambiente da AWS através de várias ferramentas. A varredura de vulnerabilidade e as práticas de remediação são revisadas regularmente como parte da conformidade contínua da AWS com o PCI DSS e o FedRAMP.
Infraestrutura e segurança de virtualização *Ambientes de produção/não*	IVS-08.1	Para sua oferta SaaS ou PaaS, vocês fornecem aos grupos de usuários 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/.

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
produção	IVS-08.2	Para sua oferta IaaS, vocês fornecem aos grupos de usuários orientações sobre como criar ambientes adequados de produção e teste?	
	IVS-08.3	Vocês separam os ambientes de produção e não produção lógica e fisicamente?	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, domínio 13 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.
Infraestrutura e segurança de virtualização *Segmentação*	IVS-09.1	Há ambientes de rede e sistema protegidos por um firewall ou firewall virtual para garantir os requisitos de segurança dos negócios e do cliente?	
	IVS-09.2	Há ambientes de rede e sistema protegidos por um firewall ou firewall virtual para garantir a conformidade com requisitos legislativos, normativos e contratuais?	
	IVS-09.3	Há ambientes de rede e sistema protegidos por um firewall ou firewall virtual para garantir a separação de ambientes de produção e não produção?	
	IVS-09.4	Há ambientes de rede e sistema protegidos por um firewall ou firewall virtual para garantir proteção e isolamento de dados confidenciais?	
Infraestrutura e segurança de virtualização *Segurança de VM - Proteção de Dados do*	IVS-10.1	Canais de comunicação protegidos e criptografados são usados ao migrar servidores físicos, aplicações ou dados para servidores virtuais?	A AWS permite que os clientes usem seus próprios mecanismos de criptografia para quase todos os serviços, incluindo S3, EBS e EC2. As sessões da VPC também são criptografadas.

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
vMotion	IVS-10.2	Vocês usam uma rede separada das redes de produção migrar servidores físicos, aplicações ou dados para servidores virtuais?	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.
Infraestrutura e segurança de virtualização *Segurança de VMM - Proteção de hypervisor*	IVS-11.1	Vocês restringem o acesso pessoal a todas as funções de gerenciamento de hypervisor ou consoles administrativos para sistemas que hospedam sistemas virtualizados com base no princípio de privilégio mínimo e têm suporte de controles técnicos (por exemplo, autenticação de dois fatores, trilhas de auditoria, filtragem de endereço IP, firewalls e comunicação encapsulada por TLS para os consoles administrativos)?	A AWS emprega o conceito de menor privilégio, permitindo somente o acesso necessário para que os usuários executem suas funções de trabalho. Quando criadas, as contas de usuário fornecem apenas o mínimo de acesso. O acesso acima desse nível exige autorização adequada. Consulte os relatórios SOC da AWS para obter mais informações sobre controles de acesso.
Infraestrutura e segurança de virtualização *Segurança sem fio*	IVS-12.1	Há políticas e procedimentos estabelecidos e mecanismos configurados e implementados para proteger o perímetro do ambiente de rede sem fio e para restringir o tráfego sem fio não autorizado?	Há políticas, procedimentos e mecanismos para proteger o ambiente de rede da AWS. Os controles de segurança da AWS são revisados por auditores externos independentes durante as nossas auditorias de conformidade com SOC, PCI DSS, ISO 27001 e FedRAMP.

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	IVS-12.2	Há políticas e procedimentos estabelecidos e mecanismos implementados, a fim de garantir que as configurações apropriadas de segurança sem fio 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)?	
	IVS-12.3	Há políticas e procedimentos estabelecidos e mecanismos implementados, a fim de proteger ambientes de rede sem fio e detectar a presença de dispositivos de rede não autorizados (invasores) para uma desconexão da rede em tempo hábil?	
Infraestrutura e segurança de virtualização *Arquitetura de rede*	IVS-13.1	Seus diagramas de arquitetura de rede identificam claramente ambientes de alto risco e fluxos de dados que podem ter impactos de conformidade legal?	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 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.

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	IVS-13.2	Vocês implementam medidas técnicas e aplicam técnicas avançadas de defesa (por exemplo, análise avançada de pacote, aceleração de tráfego e black-holing) para detecção e resposta rápida a ataques com base em rede associados a padrões anômalos de tráfego de entrada ou saída (por exemplo, spoofing de MAC e ataques de envenena-mento de ARP) e/ou ataques distribuídos de negação de serviço (DDoS)?	A segurança da AWS examina regularmente todos os endereços IP de endpoint de serviço voltados 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. Os controles de segurança da AWS são revisados por auditores externos independentes durante as nossas auditorias de conformidade com SOC, PCI DSS, ISO 27001 e FedRAMP.
Interopera-bilidade e portabilidade *APIs*	IPY-01	Vocês publicam uma lista de todas as APIs disponíveis no serviço e indicam quais são padrão e quais são personalizadas?	Detalhes sobre as APIs da AWS estão disponíveis no site da AWS em https://aws.amazon.com/documentation/. 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. Os relatórios SOC da AWS descrevem os controles vigentes para gerenciar o provisionamento a recursos da AWS. Consulte o Whitepaper de Segurança na Nuvem AWS para obter detalhes adicionais, disponível em http://aws.amazon.com/security.
Interopera-bilidade e portabilidade *Solicitação de dados*	IPY-02	Os dados não estruturados do cliente são disponibilizados mediante solicitação em um formato padrão do setor (por exemplo, .doc, .xls ou .pdf)?	
Interopera-bilidade e portabilidade *Política e Aspectos Legais*	IPY-03.1	Vocês fornecem políticas e procedimentos (isto é, acordos de nível de serviço) que regem o uso de APIs quanto à interoperabilidade entre seu serviço e aplicações de terceiros?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	IPY-03.2	Vocês fornecem políticas e procedimentos (isto é, acordos de nível de serviço) que regem a migração de dados de aplicativo de e para o seu serviço?	Os clientes mantêm o controle e a propriedade sobre seu conteúdo. Os clientes podem escolher a forma de migração de aplicações e conteúdo dentro e fora da plataforma da AWS como desejarem.
Interopera-bilidade e portabilidade *Protocolos de Rede Padronizados*	IPY-04.1	É possível importar e exportar dados e gerenciar serviços por meio de protocolos de rede padronizados seguros (por exemplo, texto não claro e autenticado) e aceitos no setor?	A AWS permite que os clientes movam os dados conforme necessário e desativem o armazenamento da AWS. Consulte http://aws.amazon.com/choosing-a-cloud-platform para obter mais informações sobre opções de armazenamento.
	IPY-04.2	Vocês fornecem aos clientes (grupos de usuários) alguma documentação que detalhe os padrões relevantes de protocolo de rede envolvidos em interoperabilidade e portabilidade?	
Interopera-bilidade e portabilidade *automatizada*	IPY-05.1	Vocês usam uma plataforma de virtualização reconhecida pelo setor e formatos de virtualização padrão (por exemplo, OVF) para ajudar a garantir a interoperabilidade?	O Amazon EC2 atualmente utiliza uma versão altamente personalizada do hypervisor Xen. O hypervisor é regularmente avaliado para verificar vulnerabilidades novas e existentes e vetores de ataque por equipes de penetração interna e externa e é bem adequado para manter um rígido isolamento entre máquinas virtuais convidadas. O hypervisor AWS Xen é regularmente avaliado por auditores independentes durante avaliações e auditorias. Consulte o Whitepaper de Segurança na Nuvem AWS para obter detalhes adicionais, disponível em http://aws.amazon.com/security.
	IPY-05.2	Vocês documentaram alterações personalizadas feitas em algum hypervisor em uso? Todos os ganchos de virtualização específicos da solução estão disponíveis para análise do cliente?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Segurança de Dispositivos Móveis *Antimalware*	MOS-01	Vocês fornecem treinamento antimalware específico para dispositivos móveis como parte do treinamento de segurança de informações?	Os procedimentos, processos e programa da AWS para gerenciar software mal-intencionado/antivírus estão em alinhamento com os padrões ISO 27001. Consulte o padrão ISO 27001, Anexo A, domínio 12 para obter mais informações.
Segurança de Dispositivos Móveis *Lojas de Aplicações*	MOS-02	Vocês documentam e disponibilizam listas de lojas de aplicativo aprovadas para dispositivos móveis que acessam ou armazenam dados da empresa e/ou sistemas da empresa?	A AWS estabeleceu políticas e uma estrutura de segurança da informação e integrou com eficácia a estrutura certificável por ISO 27001, com base em controles do ISO 27002, nos princípios de serviços de confiança do AICPA (American Institute of Certified Public Accountants), na PCI DSS v3.1 e na Publicação 800-53 do NIST (National Institute of Standards and Technology) sobre controles de segurança recomendados para sistemas de informação federais. Os clientes mantêm o controle e a responsabilidade sobre os seus dados e ativos de mídia associados. O cliente é responsável por gerenciar dispositivos móveis de segurança e o acesso à autorização do cliente.
Segurança de Dispositivos Móveis *Aplicações Aprovadas*	MOS-03	Vocês têm algum recurso de imposição de política (por exemplo, XACML) para garantir que somente aplicações aprovadas e aqueles de lojas de aplicativo aprovadas sejam carregados em um dispositivo móvel?	
Segurança de Dispositivos Móveis *Software Aprovado para BYOD*	MOS-04	A política e o treinamento de BYOD declaram claramente quais aplicações e lojas de aplicativo são aprovadas para uso em dispositivos BYOD?	
Segurança de Dispositivos Móveis *Conscienti-zação e treinamento*	MOS-05	Vocês têm uma política de dispositivos móveis documentada no treinamento de funcionários que define claramente dispositivos móveis e o uso aceitável e requisitos de dispositivos móveis?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Segurança de Dispositivos Móveis *Serviços baseados em nuvem*	MOS-06	Vocês têm uma lista documentada de serviços com base em nuvem pré-aprovados que podem ser usados para uso e armazenamento de dados comerciais da empresa por meio de um dispositivo móvel?	
Segurança de Dispositivos Móveis *Compati-bilidade*	MOS-07	Vocês têm um processo de validação de aplicativo documentado para testar problemas de compatibilidade de dispositivo, sistema operacional e aplicativo?	
Segurança de Dispositivos Móveis *Qualificação do Dispositivo*	MOS-08	Vocês têm uma política BYOD que define os dispositivos e os requisitos de qualificação permitidos para uso de BYOD?	
Segurança de Dispositivos Móveis *Inventário de Dispositivos*	MOS-09	Vocês mantêm um inventário de todos os dispositivos móveis que armazenam e acessam dados da empresa e que inclui o status do dispositivo (níveis de patch e sistema operacional, perda ou desativação, designação de dispositivo)?	
Segurança de Dispositivos Móveis *Gerencia-mento de Dispositivos*	MOS-10	Vocês têm uma solução central de gerenciamento de dispositivos móveis implantada em todos os dispositivos móveis que pode armazenar, transmitir ou processar dados da empresa?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Segurança de Dispositivos Móveis *Criptografia*	MOS-11	Sua política de dispositivos móveis exige o uso de criptografia para o dispositivo inteiro ou para dados identificados como imposição confidencial por meio de controles de tecnologia para todos os dispositivos móveis?	
Segurança de Dispositivos Móveis *Violação e Acesso à Raiz*	MOS-12.1	Sua política de dispositivos móveis proíbe a falsificação de controles de segurança incorporados em dispositivos móveis (por exemplo, violação ou acesso à raiz)?	
	MOS-12.2	Vocês têm controles de detecção e prevenção no dispositivo ou por meio de um sistema central de gerenciamento de dispositivos que proíbe a falsificação de controles de segurança integrados?	
Segurança de Dispositivos Móveis *Legal*	MOS-13.1	Sua política BYOD define claramente a expectativa de privacidade, requisitos de processo, detecção eletrônica e retenções legais?	Os clientes mantêm o controle e a responsabilidade sobre os seus dados e ativos de mídia associados. O cliente é responsável por gerenciar dispositivos móveis de segurança e o acesso à autorização do cliente.
	MOS-13.2	Vocês têm controles de detecção e prevenção no dispositivo ou por meio de um sistema central de gerenciamento de dispositivos que proíbe a falsificação de controles de segurança integrados?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Segurança de Dispositivos Móveis *Bloqueio de Tela*	MOS-14	Vocês exigem e impõem por meio de controles técnicos o bloqueio automático da tela para dispositivos BYOD e de propriedade da empresa?	
Segurança de Dispositivos Móveis *Sistemas operacionais*	MOS-15	Vocês gerenciam todas as alterações em sistemas operacionais de dispositivos móveis, níveis de patch e aplicações por meio dos processos de gerenciamento de alterações da empresa?	
Segurança de Dispositivos Móveis *Senhas*	MOS-16.1	Vocês têm políticas de senha para dispositivos móveis emitidos pela empresa e/ou dispositivos móveis BYOD?	
	MOS-16.2	Suas políticas de senha são impostas por meio de controles técnicos (isto é, MDM)?	
	MOS-16.3	Suas políticas de senha proíbem a alteração dos requisitos de autenticação (isto é, comprimento da senha/PIN) por meio de um dispositivo móvel?	
Segurança de Dispositivos Móveis *Política*	MOS-17.1	Vocês têm alguma política que exija que os usuários BYOD realizem backups de dados corporativos específicos?	
	MOS-17.2	Vocês têm alguma política que exija que os usuários BYOD proíbam o uso de lojas de aplicações não aprovadas?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	MOS-17.3	Vocês têm alguma política que exija que os usuários BYOD usem software antimalware (onde permitido)?	
Segurança de Dispositivos Móveis *Limpeza Remota*	MOS-18.1	Sua equipe de TI fornece limpeza remota ou limpeza de dados corporativos para todos os dispositivos BYOD aceitos pela empresa?	
	MOS-18.2	Sua equipe de TI fornece limpeza remota ou limpeza de dados corporativos para todos os dispositivos móveis atribuídos pela empresa?	
Segurança de Dispositivos Móveis *Patches de Segurança*	MOS-19.1	Seus dispositivos móveis têm os últimos patches relacionados à segurança disponíveis instalados na versão geral pelo fabricante do dispositivo ou pela operadora?	
	MOS-19.2	Seus dispositivos móveis permitem a validação remota para baixar os últimos patches de segurança da equipe de TI da empresa?	
Segurança de Dispositivos Móveis *Usuários*	MOS-20.1	Sua política BYOD esclarece os sistemas e servidores que podem ser usados ou acessados no dispositivo BYOD?	
	MOS-20.2	Sua política BYOD especifica as funções de usuário que podem ser acessadas por meio de um dispositivo BYOD?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Gerenciamento de Incidentes de Segurança, Detecção Eletrônica e Nuvem Forense *Manutenção de autoridade/ contato*	SEF-01.1	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. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001.
Gerenciamento de Incidentes de Segurança, Detecção Eletrônica e Nuvem Forense *Gerenciamento de incidentes*	SEF-02.1	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. A AWS foi validada e certificada por um auditor independente para confirmar o alinhamento com o padrão de certificação ISO 27001. Os relatórios SOC da AWS fornecem detalhes sobre atividades específicas de controle executadas pela AWS. Todos os dados armazenados pela AWS em nome dos clientes têm recursos sólidos de segurança e controle de isolamento de grupos de usuários. O Whitepaper de Segurança na Nuvem AWS (disponível em http://aws.amazon.com/security) fornece detalhes adicionais.
	SEF-02.2	Vocês integram exigências personalizadas de grupo de usuários aos seus planos de resposta a incidentes de segurança?	
	SEF-02.3	Vocês publicam um documento com funções e responsabilidades especificando pelo que vocês versus seus grupos de usuários são responsáveis durante incidentes de segurança?	
	SEF-02.4	Vocês testaram seus planos de resposta a incidentes de segurança no ano passado?	
Gerenciamento de Incidentes de Segurança, Detecção Eletrônica e Nuvem Forense *Relatório de incidentes*	SEF-03.1	Seu sistema de SIEM (Security Information and Event Management, Gerenciamento de eventos e informações de segurança) mescla origens de dados (logs de aplicações, logs de firewall, logs de IDS, logs de acesso físico etc.) para alertas e análise granular?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	SEF-03.2	A sua estrutura de monitoramento e registro de logs permite o isolamento de um incidente para grupos de usuários específicos?	
Gerenciamento de Incidentes de Segurança, Detecção Eletrônica e Nuvem Forense *Preparação legal de resposta a incidentes*	SEF-04.1	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?	
	SEF-04.2	O seu recurso de resposta a incidentes inclui o uso de técnicas forenses de análise e coleta de dados legalmente admissíveis?	
	SEF-04.3	Vocês são capazes de suportar suspensões por litígio (“congelamento” de dados de um ponto específico no tempo) para um grupo de usuários específico sem “congelar” dados de outros grupos de usuários?	
	SEF-04.4	Vocês aplicam e atestam separação de dados de grupos de usuários ao produzir dados em resposta a citações judiciais?	
Gerenciamento de Incidentes de Segurança, Detecção Eletrônica e Nuvem Forense	SEF-05.1	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, domínio 16 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.

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Métricas de resposta a incidentes	SEF-05.2	Vocês compartilharão dados de incidentes de segurança de informações estatísticas com seus grupos de usuários mediante solicitação?	
Gestão, Transparência e Contabilidade da Cadeia de Suprimentos *Integridade e Disponibilidade de Dados*	STA-01.1	Vocês inspecionam e se responsabilizam por erros de qualidade de dados e riscos associados, e trabalham com os seus parceiros da cadeia de suprimentos de nuvem para corrigi-los?	Os clientes mantêm o controle e a propriedade sobre a qualidade de seus dados e de erros potenciais de qualidade que podem surgir através do uso de serviços da AWS. Consulte o relatório SOC da AWS para obter detalhes específicos em relação à integridade de dados e gerenciamento de acesso (incluindo o acesso com privilégio mínimo).
	STA-01.2	Vocês projetam e implementam controles para mitigar e conter os riscos de segurança de dados através da separação adequada de funções, acesso baseado em função e acesso com menos privilégios para todo o pessoal dentro de sua cadeia de suprimentos?	
Gestão, Transparência e Contabilidade da Cadeia de Suprimentos *Relatório de incidentes*	STA-02.1	Vocês deixam as informações de incidentes de segurança disponíveis para todos os clientes afetados e prestadores periodicamente através de meios eletrônicos (por exemplo, portais)?	Os procedimentos, planos e programa de resposta a incidentes da AWS foram desenvolvidos em alinhamento com o padrão ISO 27001. Os relatórios SOC da AWS fornecem detalhes sobre atividades específicas de controle executadas pela AWS. O Whitepaper de Segurança na Nuvem AWS (disponível em http://aws.amazon.com/security) fornece detalhes adicionais.
Gestão, Transparência e Contabilidade da Cadeia de Suprimentos *Serviços de infraestrutura/ rede*	STA-03.1	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.

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	STA-03.2	Vocês fornecem aos grupos de usuários relatórios de utilização e planejamento de capacidade?	
Gestão, Transparência e Contabilidade da Cadeia de Suprimentos *Fornecedor de avaliações internas*	STA-04.1	Vocês realizam avaliações internas anuais de conformidade e eficácia de suas políticas, procedimentos e medidas de apoio e métricas?	A equipe da cadeia de suprimentos e aquisição da AWS mantém relações com todos os fornecedores da AWS. Consulte o padrão ISO 27001, Anexo A, domínio 15 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.
Gestão, Transparência e Contabilidade da Cadeia de Suprimentos *Contratos de terceiros*	STA-05.1	Vocês selecionam e monitoram provedores terceirizados em conformidade com legislações no país onde os dados são processados, armazenados e transmitidos?	Os requisitos de segurança da equipe para provedores terceirizados que oferecem suporte a sistemas e dispositivos da AWS são estabelecidos em um Acordo de Confidencialidade Mútua entre a organização pai da AWS, o Amazon.com e o respectivo provedor terceirizado. O departamento jurídico da Amazon e a equipe de aquisição da AWS definem os requisitos de segurança da equipe de provedores terceirizados da AWS em acordos de contrato com o provedor terceirizado. Todas as pessoas que trabalham com informações da AWS devem pelo menos atender ao processo de triagem para verificações de antecedentes antes da contratação e assinar um Non-Disclosure Agreement (NDA - Acordo de confidencialidade) antes de receberem acesso às informações da AWS. A AWS geralmente não terceiriza o desenvolvimento de serviços AWS a subcontratantes.
	STA-05.2	Vocês selecionam e monitoram provedores terceirizados em conformidade com legislações no país do qual os dados são originados?	
	STA-05.3	O departamento jurídico revisa todos os contratos de terceiros?	
	STA-05.4	Os acordos de terceiros incluem provisão para a segurança e proteção de informações e ativos?	
	STA-05.5	Vocês fornecem ao cliente uma lista e cópias de todos os contratos de processamento substituição e o mantêm atualizado?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
Gestão, Transparência e Contabilidade da Cadeia de Suprimentos *Avaliações de Governança da Cadeia de Suprimentos*	STA-06.1	Vocês revisam a gestão de riscos e processos de governança de parceiros para dar conta dos riscos herdados de outros membros da cadeia de suprimentos do parceiro?	A AWS mantém acordos formais com os principais fornecedores de terceiros e implementa mecanismos de gestão de relacionamento adequadas, de acordo com sua relação com o negócio. Os processos de gerenciamento de terceiros da AWS é revisado regularmente por auditores independentes, como parte da conformidade contínua da AWS com o SOC, e ISO 27001.
Gestão, Transparência e Contabilidade da Cadeia de Suprimentos *Métricas da Cadeia de Suprimentos*	STA-07.1	Políticas e procedimentos são estabelecidos, e os processos de negócios suportados e as medidas técnicas implementadas, para a manutenção de acordos completos, precisos e pertinentes (por exemplo, SLAs) entre fornecedores e clientes (grupos de usuários)?	
	STA-07.2	Vocês têm a capacidade de medir e tratar da não conformidade das disposições e/ou termos em toda a cadeia de suprimentos (upstream/ downstream)?	
	STA-07.3	Vocês podem gerenciar conflitos ou inconsistências a nível de serviço resultantes do relacionamento com fornecedores diferentes?	
	STA-07.4	Vocês revisam todos os acordos, políticas e processos ao menos uma vez ao ano?	
Gestão, Transparência e Contabilidade da Cadeia de Suprimentos *Avaliação de terceiros*	STA-08.1	Vocês garantem a segurança razoável de informações em toda a sua cadeia de suprimentos de informações através da realização de uma revisão anual?	

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
	STA-8.2	A sua revisão anual inclui todos os parceiros/ fornecedores terceirizados dos quais a sua cadeia de suprimentos de informações depende?	
Gestão, Transparência e Contabilidade da Cadeia de Suprimentos *Auditorias de terceiros*	STA-09.1	Vocês permitem que grupos de usuários realizem avaliações independentes para verificar vulnerabilidades?	Os clientes podem solicitar permissão para conduzir pesquisas de sua infraestrutura em nuvem contanto que elas se limitem a instâncias do cliente e não violem a política de uso aceitável da AWS. A prévia aprovação para esses tipos de verificações pode ser iniciada enviando-se uma solicitação por meio 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. Os relatórios SOC da AWS fornecem mais detalhes sobre atividades específicas de controle executadas pela AWS.
	STA-09.2	Vocês têm serviços terceirizados externos que realizam verificações de vulnerabilidade e testes periódicos de penetração em suas aplicações e redes?	
Gerenciamento de Vulnera-bilidades e Ameaças *Software mal-intencionado/ antivírus*	TVM-01.1	Vocês têm programas antimalware compatíveis ou que se conectam com ofertas de serviço em nuvem instalados em todos os seus sistemas?	Os procedimentos, processos e programa da AWS para gerenciar software mal-intencionado/antivírus estão em alinhamento com os padrões ISO 27001. Consulte os relatórios SOC da AWS para obter mais detalhes. Além disso, consulte o padrão ISO 27001, Anexo A, domínio 12 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.
	TVM-01.2	Vocês garantem 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?	
Gerenciamento de Vulnerabi-lidades e Ameaças *Gerenciamento de aplicação de*	TVM-02.1	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 aplicações. Além disso, são responsáveis por realizar verificações de vulnerabilidade e aplicação de correções em seus próprios sistemas. Os clientes podem solicitar

Grupo de controle	CID	Perguntas de avaliação do consenso	Resposta da AWS
correções/ vulnerabilidades	TVM-02.2	Vocês realizam verificações de vulnerabilidade na camada de aplicações regularmente, como prescrito por práticas recomendadas do setor?	permissão para conduzir pesquisas de sua infraestrutura em nuvem contanto que elas se limitem a instâncias do cliente e não violem 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 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 Segurança na Nuvem AWS para obter detalhes adicionais, disponível em http://aws.amazon.com/pt/security. Consulte o padrão ISO 27001, Anexo A, domínio 12 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.
	TVM-02.3	Vocês realizam verificações de vulnerabilidade na camada de sistemas operacionais locais regularmente, como prescrito por práticas recomendadas do setor?	
	TVM-02.4	Os resultados de verificações de vulnerabilidade estarão disponíveis para grupos de usuários mediante solicitação?	
	TVM-02.5	Vocês têm um recurso para aplicar rapidamente correções em todos os seus sistemas, aplicações e dispositivos de computação?	
	TVM-02.6	Vocês fornecerão intervalos de tempo para a aplicação de correções em sistemas, com base em riscos, para seus grupos de usuários mediante solicitação?	
Gerenciamento de Vulnerabilidades e Ameaças *Código para dispositivo móvel*	TVM-03.1	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 de acordo com suas próprias necessidades.
	TVM-03.2	Todos os códigos para dispositivos móveis não autorizados têm sua execução impedida?	

Outras fontes de leitura

Para obter informações adicionais, consulte estas fontes:

- Visão geral dos riscos e da conformidade da AWS
- Certificações, programas, relatórios e atestados de terceiros da AWS
- Respostas da AWS para as principais questões de conformidade

Revisões do documento

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