Lei Geral de Proteção de Dados do Brasil Workbook

Março 2022

[Workbook]

© 2022 Amazon Web Services, Inc. ou suas afiliadas. Todos os direitos reservados.

Avisos

Os clientes são responsáveis por fazer sua própria avaliação independente das informações neste documento. Este documento (a) é fornecido apenas para fins informativos, (b) representa as ofertas e práticas de produtos atuais da AWS, que estão sujeitas a alterações sem aviso prévio e (c) não cria nenhum compromisso ou garantia da AWS e suas afiliadas, fornecedores ou licenciadores. Os produtos ou serviços da AWS são fornecidos no “estado em que se encontram”, sem qualquer garantia, declaração ou condição de qualquer tipo, explícita ou implícita. As responsabilidades e obrigações da AWS com seus clientes são regidas por contratos da AWS, e este documento não modifica nem faz parte de nenhum contrato entre a AWS e seus clientes.

Sumário

Resumo

Este documento fornece informações sobre serviços e recursos que a Amazon Web Services (AWS) oferece aos clientes a fim de ajudá-los a estabelecer o alinhamento com os requisitos da Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira.

Esse Workbook irá:

- Ajudar os clientes a entender as respectivas funções que o cliente e a AWS desempenham no gerenciamento e na proteção do ambiente de Nuvem
- Fornecer uma visão geral das medidas de segurança recomendadas através de boas práticas, apoiando o capítulo VII “de segurança e melhores práticas” da LGPD nº 13.709 de 14 de agosto de 2018
- Fornecer considerações adicionais sobre como os clientes podem implementar medidas de segurança aplicáveis ao usar os serviços da AWS.
- Fornecer medidas de segurança recomendadas incluídas na estrutura do Center of Internet Security (CIS) versão 8.0 e seu link entre o NIST Cybersecurity Framework, o NIST Privacy Framework, o AWS Nuvem Adoption Framework e o AWS Well-Architected Framework.

Escopo

Este Workbook se concentra em perguntas típicas feitas pelos clientes da AWS quando eles estão considerando requisitos de privacidade e proteção de dados relevantes para o uso dos serviços da AWS para armazenar ou processar conteúdo que contém dados pessoais. Também haverá outras considerações relevantes para cada cliente abordar, por exemplo, a necessidade cumprir os requisitos específicos do setor, as leis de jurisdições usadas em compromissos comerciais ou contratuais que um cliente faz com terceiros.

Este documento é disponibilizado apenas para fins informativos. Não é um aconselhamento jurídico e não deve ser considerado um conselho jurídico. Como os requisitos de cada cliente serão diferentes, a AWS incentiva fortemente seus clientes a obter orientação adequada sobre a implementação de requisitos de privacidade e proteção de dados, bem como sobre as leis aplicáveis e outros requisitos relevantes para seus negócios.

Para obter mais informações sobre a estrutura de privacidade de dados do Brasil e outras considerações relevantes sobre privacidade e proteção de dados que os clientes da AWS devem considerar, visite https://aws.amazon.com/compliance/brazil-data-privacy/.

Considerações relevantes para privacidade e proteção de dados

Ao usar os serviços da AWS, cada cliente da AWS mantém a propriedade e o controle de seu conteúdo, incluindo controle sobre:

- Que conteúdo eles escolhem para armazenar ou processar usando os serviços da AWS
- Quais serviços da AWS eles usam com seu conteúdo
- A(s) região(ões) em que o conteúdo é armazenado
- O formato, a estrutura e a segurança de seu conteúdo, incluindo se está mascarado, anonimizado ou criptografado
- Quem tem acesso às contas e ao conteúdo da AWS e como esses direitos de acesso são concedidos, gerenciados e revogados

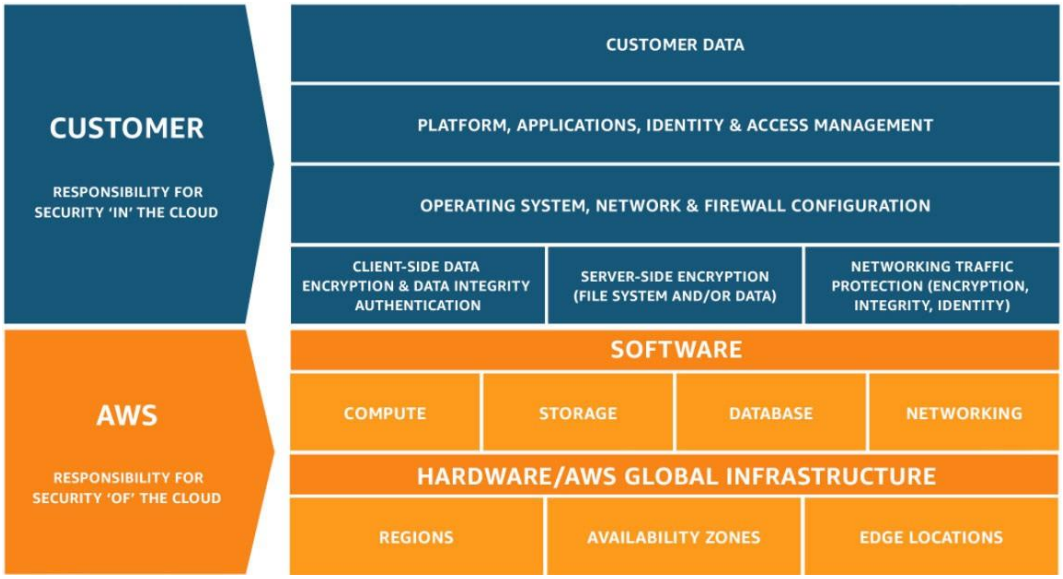
Como os clientes da AWS mantêm a propriedade e o controle sobre seu conteúdo no ambiente da AWS, eles também mantêm responsabilidades relacionadas à segurança desse conteúdo como parte do modelo de "responsabilidade compartilhada" da AWS.

Esse modelo de responsabilidade compartilhada é fundamental para entender as respectivas funções do cliente e da AWS no contexto dos requisitos de privacidade e proteção de dados que podem ser aplicados ao conteúdo que os clientes optam por armazenar ou processar usando os serviços da AWS.

Para obter informações complementares sobre como os serviços da AWS operam, incluindo como os clientes podem abordar a segurança e criptografar seu conteúdo, as localizações geográficas onde os clientes podem optar por armazenar conteúdo e outras considerações relevantes, acesse o whitepaper Como usar a AWS no contexto de considerações comuns sobre privacidade e proteção de dados

Segurança e responsabilidade compartilhada

A segurança na Nuvem é uma responsabilidade compartilhada. A AWS gerencia a segurança da Nuvem garantindo que a infraestrutura da AWS esteja em conformidade com os requisitos regulamentares globais e regionais e as melhores práticas, mas a segurança na Nuvem é responsabilidade do cliente. Os CSCs mantêm o controle dos controles de segurança que desejam implantar para proteger conteúdo, plataforma, aplicações, sistemas e redes próprios, da mesma maneira que eles fariam em um centro de dados local.



Modelo de responsabilidade compartilhada

O modelo de responsabilidade compartilhada é fundamental para entender as respectivas funções do cliente e da AWS no contexto dos princípios de segurança na Nuvem. A AWS opera, gerencia e controla os componentes da infraestrutura, desde o sistema operacional do host e da camada de virtualização até a segurança física das instalações em que os serviços são executados.

Segurança “na” Nuvem

Os clientes são responsáveis por sua segurança na Nuvem. Assim como um data center tradicional, o cliente é responsável por gerenciar o sistema operacional convidado (incluindo a instalação de atualizações e patches de segurança) e outros softwares de aplicativos associados, bem como a configuração do firewall do grupo de segurança fornecido pela AWS. Os clientes devem considerar cuidadosamente os serviços que escolherem, pois suas responsabilidades variam de acordo com os serviços que usam, a integração desses serviços em seus ambientes de TI e as leis e regulamentos aplicáveis.

É importante observar que, ao usar os serviços da AWS, os clientes mantêm o controle sobre seu conteúdo e são responsáveis pelo gerenciamento de requisitos críticos de segurança de conteúdo, incluindo:

- O conteúdo que eles escolhem armazenar na AWS
- Os serviços da AWS que são usados com o conteúdo
- O país onde o conteúdo é armazenado
- O formato e a estrutura do conteúdo e se ele está mascarado, anonimizado ou criptografado
- Como seus dados são criptografados e onde as chaves são armazenadas
- Quem tem acesso ao conteúdo e como esses direitos de acesso são concedidos, gerenciados e revogados

Como os clientes, em vez da AWS, controlam esses fatores importantes, os clientes mantêm a responsabilidade por suas escolhas. Os clientes são responsáveis pela segurança do conteúdo que colocam na AWS ou por se conectarem à infraestrutura da AWS, como o sistema operacional convidado, os aplicativos em suas instâncias de computação e o conteúdo armazenado e processado em armazenamento, plataformas, bancos de dados ou outros serviços da AWS.

Segurança “da” Nuvem

Para fornecer a segurança da Nuvem, a AWS audita continuamente seus ambientes. A infraestrutura e os serviços são aprovados para operar de acordo com vários padrões de conformidade e certificações do setor em todas as regiões e setores. Os clientes podem usar as certificações de conformidade da AWS para validar a implementação e a eficácia dos controles de segurança da AWS, incluindo as melhores práticas e certificações de segurança reconhecidas internacionalmente.

O programa de conformidade da AWS é baseado nas seguintes ações:

- **Valide** que os serviços e instalações da AWS em todo o mundo mantêm um ambiente de controle onipresente que está operando de forma eficaz. O ambiente de controles da AWS contém a mão de obra, processos e tecnologias necessários para estabelecer e manter um ambiente que apóie a eficácia operacional do framework de controles da AWS. Integramos controles específicos de Nuvem válidos definidos por organizações líderes do setor de computação em Nuvem em nosso ambiente de controle. A AWS monitora esses grupos do setor para identificar as principais práticas que podem ser implementadas e para ajudar melhor os clientes a gerenciar seu ambiente de controle.

- **Demonstramos** nossa postura de conformidade para melhor te ajudar a verificar a conformidade com os requisitos do setor e do governo. A AWS contrata órgãos externos de certificação e auditores independentes para fornecer aos clientes um grande volume de informações sobre as políticas, os processos e os controles estabelecidos. Você pode usar essas informações para executar seus procedimentos de avaliação e verificação de controles, conforme exigido pelo padrão de conformidade aplicável.

- **Monitore**, por meio do uso de milhares de requisitos de controle de segurança, que a AWS mantém a conformidade com os padrões globais e as melhores práticas.

Programas de garantia de conformidade da AWS

A AWS obteve certificações e atestados independentes de terceiros para uma variedade de cargas de trabalho específicas do setor, incluindo as seguintes:

ISO 27001 — ISO 27001 é um padrão de gerenciamento de segurança que especifica as melhores práticas de gerenciamento de segurança e controles de segurança abrangentes seguindo as orientações de práticas recomendadas da ISO 27002. A base dessa certificação é o desenvolvimento e a implementação de um programa de segurança rigoroso, que inclui o desenvolvimento e a implementação de um Sistema de Gerenciamento de Segurança da Informação que define como a AWS gerencia perpetuamente a segurança de maneira holística e abrangente. Para obter mais informações ou fazer o download da certificação ISO 27001 da AWS, consulte a página de Conformidade com a ISO 27001.

ISO 27017 — ISO 27017 fornece orientação sobre os aspectos de segurança da informação da computação em Nuvem, recomendando a implementação de controles de segurança da informação específicos da Nuvemque complementam a orientação das normas ISO 27002 e ISO 27001. Esse código de prática fornece orientações adicionais de implementação de controles de segurança da informação específicas para provedores de serviços em Nuvem. Para mais
ou para baixar a certificação ISO 27017 da AWS, consulte a página da Web de conformidade com a ISO 27017.

ISO 27018 — é um código de práticas concentrado na proteção de dados pessoais na Nuvem. Ela baseia-se no padrão de segurança da informação ISO 27002 e disponibiliza diretrizes sobre a implementação dos controles desse padrão aplicáveis às Informações Pessoalmente Identificáveis (PII) da Nuvem pública. E também fornece um conjunto de diretrizes associadas e controles adicionais destinados a abordar os requisitos de **proteção** de PII da Nuvem pública, que não foram contemplados no conjunto de controles da ISO 27002 atual. Para obter mais informações ou fazer o download da certificação ISO 27018 da AWS, consulte a página da Web de conformidade com a ISO 27018.

ISO 27701 - ISO / IEC 27701:2019 especifica requisitos e diretrizes para estabelecer e melhorar continuamente o Sistema de Gerenciamento de Informações de Privacidade (PIMS), incluindo o processamento de Informações de Identificação Pessoal (PII). É uma extensão dos padrões ISO / IEC 27001 e ISO / IEC 27002 para gerenciamento de segurança da informação, fornecendo um conjunto de controles adicionais e orientações associadas destinadas a atender aos requisitos de gerenciamento de nuvem pública PIMS e PII para processadores e controladores, não tratados pelos existentes Conjunto de controle ISO / IEC 27002. Para obter mais informações ou para baixar a certificação AWS ISO 27701, consulte a página da Web de conformidade com a ISO 27701.

ISO 9001 - ISO 9001 descreve uma abordagem orientada a processos para documentar e revisar a estrutura, responsabilidades e procedimentos necessários para alcançar uma gestão de qualidade eficaz dentro de uma organização. A chave para a certificação contínua sob esse padrão é estabelecer, manter e melhorar a estrutura organizacional, as responsabilidades, os procedimentos, os processos e os recursos de uma maneira em que os produtos e serviços da AWS satisfaçam consistentemente os requisitos de qualidade da ISO 9001. Para obter mais informações ou fazer o download da certificação ISO 9001 da AWS, consulte a página da Web de conformidade com a ISO 9001.

PCI DSS Nível 1 - O Padrão de Segurança de Dados do Setor de Cartões de Pagamento (também conhecido como PCI DSS) é um padrão proprietário de segurança de informações administrado pelo PCI Security Standards Council.
O PCI DSS é aplicável a todas as entidades que armazenam, processam ou transmitem dados de portadores de cartões (CHD – Card Holder Data) e/ou dados sigilosos de autenticação (SAD – Sensitive Authentication Data), incluindo comerciantes, processadores, compradores, emissores e provedores de serviços. O PCI DSS é mandatado pelas marcas de cartão e administrado pelo Payment Card Industry Security Standards Council. Para obter mais informações ou para solicitar o Resumo de Atestado de Conformidade e Responsabilidade do PCI DSS, consulte a página da Web de Conformidade com o PCI DSS.

Os relatórios do AWS SOC são frutos de análises independentes de terceiros que demonstram como a AWS obtém controles e objetivos de conformidade chave. O objetivo desses relatórios é ajudar os clientes e seus auditores a entender os controles da AWS estabelecidos para apoiar as operações e a conformidade. Para obter mais informações, consulte a página da Web de Conformidade SOC. Existem três tipos de relatórios do AWS SOC:

- **SOC 1:** fornece informações sobre o ambiente de controle da AWS que podem ser relevantes para os controles internos de um cliente sobre relatórios financeiros, bem como informações para avaliação e opinião sobre a eficácia dos controles internos sobre relatórios financeiros (ÍCONE).
- **SOC 2:** fornece aos clientes e seus usuários de serviços uma necessidade comercial com uma avaliação independente do ambiente de controle da AWS relevante para a segurança, a disponibilidade e a confidencialidade do sistema.
- **SOC 3:** fornece aos clientes e seus usuários de serviços uma necessidade comercial com uma avaliação independente do ambiente de controle da AWS relevante para a segurança, a disponibilidade e a confidencialidade do sistema sem divulgar a AWS interna informação.

CISPE – A CISPE(Provedores de serviços de infraestrutura de nuvem da Europa) é uma coalização de empresas líderes em computação em nuvem que atende a milhões de clientes europeus. A CISPE desenvolveu, em colaboração com a CNIL (Autoridade francesa de proteção dos dados), o Código de conduta para proteção de dados da CISPE (Código da CISPE), o primeiro código de conduta pan-europeu para proteção dos dados focado em serviços de infraestrutura em nuvem. O Código da CISPE é endossado pelo Conselho Europeu de Proteção de Dados e aprovado pela CNIL.

O Código da CISPE ajuda os clientes a garantir que seu provedor de serviços de infraestrutura de nuvem ofereça garantias operacionais adequadas para demonstrar conformidade com o Regulamento Geral sobre a Proteção de Dados (RGPD) e proteger os dados dos clientes. Para obter mais informações, consulte a página da Web de Conformidade CISPE.

Ao integrar recursos de serviços com foco em governança e facilmente auditáveis a padrões de auditoria ou conformidade aplicáveis, os capacitadores de conformidade da AWS aproveitam os programas tradicionais, ajudando clientes a estabelecerem e operarem em um ambiente de controle de segurança da AWS.

Para obter mais informações sobre outras certificações e atestados da AWS, consulte a página do AWS Assurance Programs. Para obter informações sobre os controles gerais de segurança da AWS e a segurança específica do serviço, consulte o whitepaper Amazon Web Services: Overview of Security Processes.

AWS Artifact

Os clientes podem analisar e baixar relatórios e detalhes sobre mais de 2.600 controles de segurança usando o AWS Artifact, o portal automatizado de relatórios de conformidade disponível no Console de Gerenciamento da AWS. Os relatórios disponíveis no AWS Artifact incluem nossos relatórios de controle de organização de serviços (SOC), relatórios do setor de cartões de pagamento (PCI) e certificações de órgãos de acreditação em regiões geográficas e verticais de conformidade que validam a implementação e a eficácia operacional dos controles de segurança da AWS. Os contratos disponíveis no AWS Artifact incluem o Business Associate Addendum (BAA) e o Acordo de confidencialidade (NDA).

Brasil — Lei Geral de Proteção de Dados — Boas Práticas de Segurança

A Lei Geral de Proteção de Dados do Brasil ("LGPD") é a principal regulamentação do Brasil voltada para a proteção de dados pessoais passou a vigorar em Agosto de 2020. A LGPD se aplica ao tratamento de dados pessoais (definidos como informações referentes a uma pessoa física identificada ou identificável) realizado por pessoas físicas ou jurídicas do setor público ou privado, independentemente dos meios utilizados para o tratamento ou do país em que o controlador ou os dados estejam localizados, desde que: 1) o tratamento seja realizado no Brasil, 2) o tratamento seja destinado à oferta ou fornecimento de bens ou serviços, ou ao tratamento de dados de pessoas localizadas no Brasil, ou 3) os dados pessoais tenham sido coletados no Brasil.
A LGPD estabelece princípios e regras para o processamento de dados pessoais. As organizações devem demonstrar a adoção de medidas capazes de comprovar a conformidade com as regras de proteção de dados pessoais, incluindo a eficácia dessas medidas, exigindo a criação e a aplicação de políticas compatíveis aplicáveis ao processamento de dados pessoais.
Sob a LGPD, os controladores e operadores (conforme definido na LGPD) são obrigados a adotar medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilegais de destruição, perda, alteração, comunicação ou qualquer tipo de atividade de tratamento imprópria ou ilegal. Além disso, a LGPD concede à Autoridade Nacional de Proteção de Dados ("ANPD") autoridade para estabelecer padrões técnicos mínimos a serem implementados por controladores e operadores.

Em abril de 2021, o Governo Brasileiro emitiu o Guia de Framework de Segurança relacionado às medidas de segurança para apoiar as empresas na implementação de controles que ajudarão a proteger dados pessoais e atenderão à LGPD nº 13.709 Capítulo VII “de segurança e melhores práticas”. O guia conta com os frameworks Center for Internet Security (CIS) e NIST Cybersecurity.

De maneira a suportar nossos clientes com requisitos de compliance da LGPD usando serviços da AWS, criamos um workbook de boas práticas. As tabelas abaixo listam cada uma das **medidas de segurança recomendadas** incluídas na versão 8.0 da estrutura do Center for Internet Security (CIS), que também mapeia onde cada controle atende ao NIST Cybersecurity Frameworke fornece considerações adicionais sobre como os clientes da AWS podem implementar quaisquer medidas de segurança aplicáveis ao usar os serviços da AWS, suportando o capítulo VII “da segurança e boas práticas” da LGPD.

Os clientes também podem acessar materiais de apoio sobre NIST Cybersecurity Framework na página de Compliance.

Essas tabelas contêm apenas uma amostra não exaustiva de considerações. Isso não é um conselho legal ou de conformidade, os clientes devem consultar suas próprias equipes jurídicas e de conformidade.

Controle	ID	NIST CSF	Detalhes do controle CIS	Responsabilidades		Considerações da AWS
				AWS	Cliente	
Inventário e controle de ativos corporativos	1.1	Identificar	Estabelecer e manter um inventário preciso, detalhado e atualizado de todos os ativos corporativos com potencial para armazenar ou processar dados, incluindo: dispositivos de usuário final (incluindo portáteis e móveis), dispositivos de rede, dispositivos não computacionais/IoT e servidores. Certifique-se de que o inventário registre o endereço de rede (se estático), o endereço de hardware, o nome da máquina, o proprietário do ativo de dados, o departamento de cada ativo e se o ativo foi aprovado para se conectar à	AWS	Cliente	N/A — Os clientes não têm nenhuma responsabilidade na Nuvem AWS pelo inventário de dispositivos e sistemas físicos da AWS. Os clientes são responsáveis apenas por esse controle dos ativos físicos que possuem e operam fora da nuvem (por exemplo, servidores, computadores, equipamentos de rede, dispositivos móveis, dispositivos IoT, periféricos, etc.). Os clientes da AWS são responsáveis por desenvolver, documentar, revisar e atualizar, com uma frequência definida pela organização, um inventário de componentes de software para seus sistemas hospedados na AWS. Os clientes da AWS são responsáveis por verificar se o inventário: 1) reflete com precisão o sistema atual, 2) Inclui todos os componentes dentro do limite de autorização, 3) Está no nível de granularidade considerado necessário para rastreamento e geração de relatórios e 4) Inclui as informações prescritas pela configuração política de gestão que é considerada necessária para alcançar a responsabilidade efetiva dos componentes do sistema de informação.

			rede. Para dispositivos móveis de usuário final, as ferramentas do tipo MDM podem oferecer suporte a esse processo, quando apropriado. Esse inventário inclui ativos conectados à infraestrutura física, virtual, remotamente e aqueles em ambientes de Cloud. Além disso, inclui ativos que são regularmente conectados à infraestrutura de rede da empresa, mesmo que não estejam sob controle da empresa. Revise e atualize o inventário de todos os ativos corporativos semestralmente ou com mais frequência.			
Inventário e controle de ativos corporativos	1.2	Responder	Certifique-se de que exista um processo para tratar ativos não autorizados semanalmente. A empresa pode optar por remover	AWS	Cliente	N/A — Os clientes não têm nenhuma responsabilidade na Nuvem AWS pelo inventário de dispositivos e sistemas físicos da AWS. Os clientes são responsáveis apenas por esse controle dos ativos físicos que possuem e operam fora da nuvem (por exemplo, servidores, computadores, equipamentos de rede, dispositivos móveis, dispositivos IoT, periféricos, etc.).

			o ativo da rede, negar que o ativo se conecte remotamente à rede ou colocar o ativo em quarentena.			Os clientes da AWS são responsáveis por desenvolver, documentar, revisar e atualizar, com uma frequência definida pela organização, um inventário de componentes de software para seus sistemas hospedados na AWS. Os clientes da AWS são responsáveis por verificar se o inventário: 1) reflete com precisão o sistema atual, 2) Inclui todos os componentes dentro do limite de autorização, 3) Está no nível de granularidade considerado necessário para rastreamento e geração de relatórios e 4) Inclui as informações prescritas pela configuração política de gestão que é considerada necessária para alcançar a responsabilidade efetiva dos componentes do sistema de informação.
Inventário e controle de ativos corporativos	1.3	Detectar	Utilize uma ferramenta de descoberta ativa para identificar ativos conectados à rede da empresa. Configure a ferramenta de descoberta ativa para ser executada diariamente ou com mais frequência.	AWS	Cliente	N/A — Os clientes não têm nenhuma responsabilidade na Nuvem AWS pelo inventário de dispositivos e sistemas físicos da AWS. Os clientes são responsáveis apenas por esse controle dos ativos físicos que possuem e operam fora da nuvem (por exemplo, servidores, computadores, equipamentos de rede, dispositivos móveis, dispositivos IoT, periféricos, etc.). Os clientes da AWS são responsáveis por desenvolver, documentar, revisar e atualizar, com uma frequência definida pela organização, um inventário de componentes de software para seus sistemas hospedados na AWS. Os clientes da AWS são responsáveis por verificar se o inventário: 1) reflete com precisão o sistema atual, 2) Inclui todos os componentes dentro do limite de autorização, 3) Está no nível de granularidade considerado necessário para rastreamento e geração de relatórios e 4) Inclui as informações prescritas pela configuração política de gestão que é considerada necessária para alcançar a responsabilidade efetiva dos componentes do sistema de informação.
Inventário e controle de ativos corporativos	1.4	Identificar	Use o log DHCP em todos os servidores DHCP ou ferramentas de gerenciamento de endereço IP (Internet Protocol) para atualizar o inventário de ativos da empresa. Revise e use registros para atualizar o inventário de	AWS	Cliente	N/A — Os clientes não têm nenhuma responsabilidade na Nuvem AWS pelo inventário de dispositivos e sistemas físicos da AWS. Os clientes são responsáveis apenas por esse controle dos ativos físicos que possuem e operam fora da nuvem (por exemplo, servidores, computadores, equipamentos de rede, dispositivos móveis, dispositivos IoT, periféricos, etc.). Os clientes da AWS são responsáveis por desenvolver, documentar, revisar e atualizar, com uma frequência definida pela organização, um inventário de componentes de software para seus sistemas hospedados na AWS. Os clientes da AWS são responsáveis por verificar se o inventário: 1) reflete com precisão o sistema atual, 2) Inclui todos os componentes dentro do limite de autorização, 3) Está no nível de granularidade considerado necessário para

			ativos da empresa semanalmente ou com mais frequência.			rastreamento e geração de relatórios e 4) Inclui as informações prescritas pela configuração política de gestão que é considerada necessária para alcançar a responsabilidade efetiva dos componentes do sistema de informação. Os clientes também podem consultar este guia de DHCP para configurar seu ambiente na Nuvem AWS.
Inventário e controle de ativos corporativos	1.5	Detectar	Use uma ferramenta de descoberta passiva para identificar ativos conectados à rede da empresa. Revise e use varreduras para atualizar o inventário de ativos da empresa pelo menos uma vez por semana ou com mais frequência.	AWS	Cliente	N/A — Os clientes não têm nenhuma responsabilidade na Nuvem AWS pelo inventário de dispositivos e sistemas físicos da AWS. Os clientes são responsáveis apenas por esse controle dos ativos físicos que possuem e operam fora da nuvem (por exemplo, servidores, computadores, equipamentos de rede, dispositivos móveis, dispositivos IoT, periféricos, etc.). Os clientes da AWS são responsáveis por desenvolver, documentar, revisar e atualizar, com uma frequência definida pela organização, um inventário de componentes de software para seus sistemas hospedados na AWS. Os clientes da AWS são responsáveis por verificar se o inventário: 1) reflete com precisão o sistema atual, 2) Inclui todos os componentes dentro do limite de autorização, 3) Está no nível de granularidade considerado necessário para rastreamento e geração de relatórios e 4) Inclui as informações prescritas pela configuração política de gestão que é considerada necessária para alcançar a responsabilidade efetiva dos componentes do sistema de informação.
Inventário e controle de ativos de software	2.1	Identificar	Estabelecer e manter um inventário detalhado de todos os softwares licenciados instalados nos ativos corporativos. O inventário de software deve documentar o título, o editor, a data inicial de instalação/uso e a finalidade comercial de cada	AWS	Cliente	N/A — Os clientes não têm nenhuma responsabilidade na Nuvem AWS pelo inventário de dispositivos e sistemas físicos da AWS. Os clientes são responsáveis apenas por esse controle dos ativos físicos que possuem e operam fora da nuvem (por exemplo, servidores, computadores, equipamentos de rede, dispositivos móveis, dispositivos IoT, periféricos, etc.). Os clientes da AWS são responsáveis por desenvolver, documentar, revisar e atualizar, com uma frequência definida pela organização, um inventário de componentes de software para seus sistemas hospedados na AWS. Os clientes da AWS são responsáveis por verificar se o inventário: 1) reflete com precisão o sistema atual, 2) Inclui todos os componentes dentro do limite de autorização, 3) Está no nível de granularidade considerado necessário para rastreamento e geração de relatórios e 4) Inclui as informações prescritas pela configuração política de gestão que é considerada necessária para alcançar a responsabilidade efetiva dos componentes do sistema de informação.

			entrada; quando apropriado, incluir o URL (Uniform Resource Locator), a (s) loja (s) de aplicativos, a (s) versão (ões), o mecanismo de implantação e a data de desativação. Revise e atualize o inventário de software semestralmente ou com mais frequência.			
Inventário e controle de ativos de software	2.2	Identificar	Certifique-se de que somente o software suportado atualmente seja designado como autorizado no inventário de software para ativos corporativos. Se o software não for suportado, mas necessário para o cumprimento da missão da empresa, documente uma exceção detalhando os controles atenuantes e a aceitação do risco residual. Para qualquer software não suportado	AWS	Cliente	N/A — Os clientes não têm nenhuma responsabilidade na Nuvem AWS pelo inventário de dispositivos e sistemas físicos da AWS. Os clientes são responsáveis apenas por esse controle dos ativos físicos que possuem e operam fora da nuvem (por exemplo, servidores, computadores, equipamentos de rede, dispositivos móveis, dispositivos IoT, periféricos, etc.). Os clientes da AWS são responsáveis por desenvolver, documentar, revisar e atualizar, com uma frequência definida pela organização, um inventário de componentes de software para seus sistemas hospedados na AWS. Os clientes da AWS são responsáveis por verificar se o inventário: 1) reflete com precisão o sistema atual, 2) Inclui todos os componentes dentro do limite de autorização, 3) Está no nível de granularidade considerado necessário para rastreamento e geração de relatórios e 4) Inclui as informações prescritas pela configuração política de gestão que é considerada necessária para alcançar a responsabilidade efetiva dos componentes do sistema de informação.

			sem uma documentação de exceção, designe como não autorizado. Revise a lista de software para verificar o suporte de software pelo menos uma vez por mês ou com mais frequência.			
Inventário e controle de ativos de software	2.3	Responder	Certifique-se de que o software não autorizado seja removido do uso em ativos corporativos ou receba uma exceção documentada. Analise mensalmente ou com mais frequência.	AWS	Cliente	N/A — Os clientes não têm nenhuma responsabilidade na Nuvem AWS pelo inventário de dispositivos e sistemas físicos da AWS. Os clientes são responsáveis apenas por esse controle dos ativos físicos que possuem e operam fora da nuvem (por exemplo, servidores, computadores, equipamentos de rede, dispositivos móveis, dispositivos IoT, periféricos, etc.). Os clientes da AWS são responsáveis por desenvolver, documentar, revisar e atualizar, com uma frequência definida pela organização, um inventário de componentes de software para seus sistemas hospedados na AWS. Os clientes da AWS são responsáveis por verificar se o inventário: 1) reflete com precisão o sistema atual, 2) Inclui todos os componentes dentro do limite de autorização, 3) Está no nível de granularidade considerado necessário para rastreamento e geração de relatórios e 4) Inclui as informações prescritas pela configuração política de gestão que é considerada necessária para alcançar a responsabilidade efetiva dos componentes do sistema de informação.
Inventário e controle de ativos de software	2.4	Detectar	Utilize ferramentas de inventário de software, quando possível, em toda a empresa para automatizar a descoberta e a documentação do software instalado.	AWS	Cliente	N/A — Os clientes não têm nenhuma responsabilidade na Nuvem AWS pelo inventário de dispositivos e sistemas físicos da AWS. Os clientes são responsáveis apenas por esse controle dos ativos físicos que possuem e operam fora da nuvem (por exemplo, servidores, computadores, equipamentos de rede, dispositivos móveis, dispositivos IoT, periféricos, etc.). Os clientes da AWS são responsáveis por desenvolver, documentar, revisar e atualizar, com uma frequência definida pela organização, um inventário de componentes de software para seus sistemas hospedados na AWS. Os

						clientes da AWS são responsáveis por verificar se o inventário: 1) reflete com precisão o sistema atual, 2) Inclui todos os componentes dentro do limite de autorização, 3) Está no nível de granularidade considerado necessário para rastreamento e geração de relatórios e 4) Inclui as informações prescritas pela configuração política de gestão que é considerada necessária para alcançar a responsabilidade efetiva dos componentes do sistema de informação.
Inventário e controle de ativos de software	2.5	Proteger	Use controles técnicos, como lista de permissões de aplicativos, para garantir que somente o software autorizado possa ser executado ou acessado. Reavalie semestralmente ou com mais frequência.	AWS	Cliente	N/A — Os clientes não têm nenhuma responsabilidade na Nuvem AWS pelo inventário de dispositivos e sistemas físicos da AWS. Os clientes são responsáveis apenas por esse controle dos ativos físicos que possuem e operam fora da nuvem (por exemplo, servidores, computadores, equipamentos de rede, dispositivos móveis, dispositivos IoT, periféricos, etc.). Os clientes da AWS são responsáveis por desenvolver, documentar, revisar e atualizar, com uma frequência definida pela organização, um inventário de componentes de software para seus sistemas hospedados na AWS. Os clientes da AWS são responsáveis por verificar se o inventário: 1) reflete com precisão o sistema atual, 2) Inclui todos os componentes dentro do limite de autorização, 3) Está no nível de granularidade considerado necessário para rastreamento e geração de relatórios e 4) Inclui as informações prescritas pela configuração política de gestão que é considerada necessária para alcançar a responsabilidade efetiva dos componentes do sistema de informação.
Inventário e controle de ativos de software	2.6	Proteger	Use controles técnicos para garantir que apenas bibliotecas de software autorizadas, como arquivos.dll, .ocx, .so, etc., específicos, tenham permissão para carregar em um processo do sistema. Impeça que bibliotecas não autorizadas sejam carregadas em um processo	AWS	Cliente	N/A — Os clientes não têm nenhuma responsabilidade na Nuvem AWS pelo inventário de dispositivos e sistemas físicos da AWS. Os clientes são responsáveis apenas por esse controle dos ativos físicos que possuem e operam fora da nuvem (por exemplo, servidores, computadores, equipamentos de rede, dispositivos móveis, dispositivos IoT, periféricos, etc.). Os clientes da AWS são responsáveis por desenvolver, documentar, revisar e atualizar, com uma frequência definida pela organização, um inventário de componentes de software para seus sistemas hospedados na AWS. Os clientes da AWS são responsáveis por verificar se o inventário: 1) reflete com precisão o sistema atual, 2) Inclui todos os componentes dentro do limite de autorização, 3) Está no nível de granularidade considerado necessário para rastreamento e geração de relatórios e 4) Inclui as informações prescritas pela configuração política de gestão que é considerada necessária para alcançar a responsabilidade efetiva dos componentes do sistema de informação.

			do sistema. Reavalie semestralmente ou com mais frequência.			
Inventário e controle de ativos de software	2.7	Proteger	Use controles técnicos, como assinaturas digitais e controle de versão, para garantir que apenas scripts autorizados, como arquivos.ps1, .py, etc., específicos, tenham permissão para executar. Impeça a execução de scripts não autorizados. Reavalie semestralmente ou com mais frequência.	AWS	Cliente	N/A — Os clientes não têm nenhuma responsabilidade na Nuvem AWS pelo inventário de dispositivos e sistemas físicos da AWS. Os clientes são responsáveis apenas por esse controle dos ativos físicos que possuem e operam fora da nuvem (por exemplo, servidores, computadores, equipamentos de rede, dispositivos móveis, dispositivos IoT, periféricos, etc.). Os clientes da AWS são responsáveis por desenvolver, documentar, revisar e atualizar, com uma frequência definida pela organização, um inventário de componentes de software para seus sistemas hospedados na AWS. Os clientes da AWS são responsáveis por verificar se o inventário: 1) reflete com precisão o sistema atual, 2) Inclui todos os componentes dentro do limite de autorização, 3) Está no nível de granularidade considerado necessário para rastreamento e geração de relatórios e 4) Inclui as informações prescritas pela configuração política de gestão que é considerada necessária para alcançar a responsabilidade efetiva dos componentes do sistema de informação.
Proteção de dados	3.1	Identificar	Estabelecer e manter um processo de gerenciamento de dados. No processo, trate da confidencialidade dos dados, do proprietário dos dados, do tratamento dos dados, dos limites de retenção de dados e dos requisitos de		Cliente	Os clientes mantêm o controle e são responsáveis por seus dados, controles de segurança, exclusão e procedimentos de suporte. Somente o cliente sabe por que os dados pessoais incluídos no conteúdo do cliente armazenado na AWS foram coletados, e somente o cliente sabe quando não é mais necessário reter esses dados pessoais para fins legítimos. O cliente deve excluir ou anonimizar os dados pessoais quando não forem mais necessários. Para obter mais informações sobre o ciclo de vida dos dados, consulte nosso whitepaper “Como usar a AWS no contexto de considerações comuns sobre privacidade e proteção de dados”

			eliminação, com base nos padrões de confidencialidade e retenção para a empresa. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças corporativas significativas que possam afetar essa Proteção.			Os serviços da AWS fornecem ao cliente controles para permitir que o cliente exclua conteúdo, conforme descrito na documentação da AWS (https://aws.amazon.com/documentation/).
Proteção de dados	3.2	Identificar	Estabelecer e manter um inventário de dados, com base no processo de gerenciamento de dados da empresa. Dados confidenciais de inventário, no mínimo. Revise e atualize o inventário anualmente, no mínimo, com prioridade em dados confidenciais.		Cliente	Os clientes mantêm o controle e são responsáveis por seus dados, controles de segurança, exclusão e procedimentos de suporte. Somente o cliente sabe por que os dados pessoais incluídos no conteúdo do cliente armazenado na AWS foram coletados, e somente o cliente sabe quando não é mais necessário reter esses dados pessoais para fins legítimos. O cliente deve excluir ou anonimizar os dados pessoais quando não forem mais necessários. Para obter mais informações sobre o ciclo de vida dos dados, consulte nosso whitepaper “Como usar a AWS no contexto de considerações comuns sobre privacidade e proteção de dados”.
Proteção de dados	3.3	Proteger	Configure listas de controle de acesso a dados com base na necessidade de um usuário saber. Aplique listas de controle de acesso		Cliente	A AWS oferece aos clientes a capacidade de configurar e usar adequadamente as ofertas de serviços da AWS para manter a segurança, a proteção e o backup adequados dos dados dos clientes. O AWS Identity and Access Management (IAM) permite que os clientes controlem com segurança o acesso aos serviços e recursos da AWS para

			a dados, também conhecidas como permissões de acesso, a sistemas de arquivos, bancos de dados e aplicativos locais e remotos.			seus usuários. Informações adicionais sobre o IAM podem ser encontradas em nosso site em https://aws.amazon.com/iam/. Estratégias para gerenciar usuários, grupos, funções e conceder acesso a dados de clientes podem ser encontradas no whitepaper Práticas recomendadas de segurança da AWS (https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf), na seção Gerenciar contas da AWS, usuários, grupos e funções do IAM.
Proteção de dados	3.4	Proteger	Retenha dados de acordo com o processo de gerenciamento de dados da empresa. A retenção de dados deve incluir cronogramas mínimos e máximos.		Cliente	A AWS oferece aos clientes a capacidade de configurar e usar adequadamente as ofertas de serviços da AWS para manter a segurança, a proteção e o backup adequados dos dados dos clientes. A AWS permite que os clientes realizem seus próprios backups usando serviços como o AWS Backup, que é um serviço de backup totalmente gerenciado que simplifica a centralização e a automatização do backup de dados nos serviços da AWS na Cloud e no local usando o AWS Storage Gateway. Usando o AWS Backup, os clientes podem configurar centralmente políticas de backup e monitorar atividades de backup para recursos da AWS, como volumes do Amazon EBS, bancos de dados do Amazon RDS, tabelas do Amazon DynamoDB, sistemas de arquivos do Amazon EFS e volumes do AWS Storage Gateway. O AWS Backup automatiza e consolida tarefas de backup executadas anteriormente serviço por serviço, eliminando a necessidade de criar scripts personalizados e processos manuais. Com apenas alguns cliques no console do AWS Backup, os clientes podem criar políticas de backup que automatizam as agendas de backup e o gerenciamento de retenção. O AWS Backup oferece uma solução de backup totalmente gerenciada e baseada em políticas, simplificando o gerenciamento de backup, ajudando que você atenda aos requisitos de conformidade de backup normativos e de negócios. Para obter mais informações, consulte o whitepaper sobre abordagens de backup e recuperação usando a AWS, disponível em https://d0.awsstatic.com/whitepapers/Backup_and_Recovery_Approaches_Using_AWS.pdf
Proteção de dados	3.5	Proteger	Descarte os dados com segurança, conforme descrito	AWS	Cliente	Os clientes mantêm o controle e são responsáveis por seus dados, controles de segurança, exclusão e procedimentos de suporte.

			no processo de gerenciamento de dados da empresa. Certifique-se de que o processo e o método de descarte sejam compatíveis com a sensibilidade dos dados.			Os serviços da AWS fornecem ao cliente controles para permitir que o cliente exclua conteúdo, conforme descrito na documentação da AWS (https://aws.amazon.com/documentation/). Em alinhamento com os padrões ISO 27001, quando um dispositivo de armazenamento da AWS atinge o fim de sua vida útil, os procedimentos da AWS incluem um processo de desativação projetado para impedir que os dados do cliente sejam expostos a indivíduos não autorizados. A AWS usa as técnicas detalhadas no NIST 800-88 (“Guidelines for Media Sanitization”) como parte do processo de desativação.
Proteção de dados	3.6	Proteger	Criptografe dados em dispositivos de usuário final que contêm dados confidenciais. Exemplos de implementações podem incluir: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.		Cliente	Os clientes da AWS assumem a responsabilidade e o gerenciamento da segurança do dispositivo do usuário final, incluindo aplicação de patches, criptografia de dados e registro em log.
Proteção de dados	3.7	Identificar	Estabelecer e manter um esquema geral de classificação de dados para a empresa. As empresas podem usar rótulos, como “Confidencial”, “Confidencial” e “Público”, e classificar seus dados de acordo com esses rótulos. Revise e atualize o esquema de	AWS	Cliente	A AWS trata todo o conteúdo do cliente e os ativos associados como altamente confidenciais. Os serviços da Cloud AWS são independentes de conteúdo, pois oferecem o mesmo alto nível de segurança a todos os clientes, independentemente do tipo de conteúdo que está sendo armazenado. Estamos atentos à segurança de nossos clientes e implementamos medidas técnicas e físicas sofisticadas contra acesso não autorizado. A AWS não tem insights sobre o tipo de conteúdo que o cliente escolhe armazenar na AWS, e o cliente mantém o controle total de como escolhe classificar seu conteúdo, onde é armazenado, como é usado e como é protegido contra divulgação. A AWS publicou um whitepaper de classificação de dados que descreve um processo por meio do qual os clientes podem criar seu próprio programa de classificação de dados https://docs.aws.amazon.com/whitepapers/latest/data-classification/welcome.html.

			classificação anualmente ou quando ocorrerem mudanças significativas na empresa que possam afetar essa Salvaguarda.			
Proteção de dados	3.8	Identificar	Fluxos de dados do documento A documentação do fluxo de dados inclui fluxos de dados do provedor de serviços e deve ser baseada no processo de gerenciamento de dados da empresa. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças corporativas significativas que possam afetar essa Proteção.	AWS	Cliente	A AWS definiu listas de controle de acesso (ACLs) de rede. A AWS desenvolveu, documentou e mantém um inventário de sistemas e dispositivos que inclui os seguintes atributos: - Nome do host - Endereço IP - Fabricante - Tipo - Modelo - Número de série - Etiqueta de ativo - Localização (inclui data center, rack e slot para rack) - Informações de licença de software (quando aplicável) - Proprietário financeiro Os clientes da AWS são responsáveis por desenvolver, documentar, revisar e atualizar, com uma frequência definida pela organização, um inventário e um fluxo de dados dos componentes do sistema para seus sistemas.
Proteção de dados	3.9	Proteger	Criptografar dados em mídia removível.		Cliente	Os clientes podem escolher como seu conteúdo é protegido. A AWS oferece recursos de criptografia para ajudar a proteger o conteúdo do cliente em trânsito e em repouso, além de oferecer aos clientes a opção de gerenciar suas próprias chaves de criptografia. Esses recursos de proteção de dados incluem: — Recursos de criptografia de dados disponíveis em mais de 100 serviços da AWS.— Opções flexíveis de gerenciamento de chaves usando o AWS Key Management Service (KMS), permitindo que os clientes escolham se a AWS gerencia suas chaves de criptografia ou permite que os clientes mantenham controle total sobre suas chaves.
	3.1	Proteger			Cliente	

Proteção de dados			Criptografe dados confidenciais em trânsito. Exemplos de implementações podem incluir: Transport Layer Security (TLS) e Open Secure Shell (OpenSSH).			O cliente determina e controla o motivo pelo qual coleta dados pessoais, para que serão usados, para quem podem ser usados e para quem são divulgados. A AWS fornece endpoints HTTPS usando o protocolo Transport Layer Security (TLS, Camada de segurança de transporte) para comunicação, o que concede a você criptografia em trânsito quando usa as APIs da AWS. Use o serviço de AWS Certificate Manager (ACM) para criar, gerenciar e implantar os certificados privados e públicos que você utiliza para estabelecer um transporte criptografado das cargas de trabalho entre sistemas. O Amazon Elastic Load Balancing está integrado ao ACM e é usado como suporte para os protocolos HTTPS.
Proteção de dados	3.11	Proteger	Criptografe dados confidenciais em repouso em servidores, aplicativos e bancos de dados que contêm dados confidenciais. A criptografia da camada de armazenamento, também conhecida como criptografia do lado do servidor, atende aos requisitos mínimos desse Safeguard. Métodos de criptografia adicionais podem incluir criptografia na camada do aplicativo, também conhecida como criptografia do lado do cliente, em que o acesso ao (s) dispositivo (s) de		Cliente	Os clientes podem escolher como seu conteúdo é protegido. A AWS oferece recursos de criptografia para ajudar a proteger o conteúdo do cliente em trânsito e em repouso, além de oferecer aos clientes a opção de gerenciar suas próprias chaves de criptografia. Esses recursos de proteção de dados incluem: — Recursos de criptografia de dados disponíveis em mais de 100 serviços da AWS.— Opções flexíveis de gerenciamento de chaves usando o AWS Key Management Service (KMS), permitindo que os clientes escolham se a AWS gerencia suas chaves de criptografia ou permite que os clientes mantenham controle total sobre suas chaves.

			armazenamento de dados não permite o acesso aos dados de texto simples.			
Proteção de dados	3.12	Proteger	Segmente o processamento e o armazenamento de dados com base na sensibilidade dos dados. Não processe dados confidenciais em ativos corporativos destinados a dados de menor confidencialidade.	AWS	Cliente	Os clientes da AWS devem arquitetar seu uso da AWS para aproveitar as vantagens de várias regiões e zonas de disponibilidade. A distribuição de aplicativos em várias zonas de disponibilidade oferece a capacidade de permanecer resiliente diante da maioria dos modos de falha, incluindo desastres naturais ou falhas do sistema. A infraestrutura da AWS tem um alto nível de disponibilidade e oferece aos clientes os recursos para implantar uma arquitetura de TI resiliente. Nossos sistemas são projetados para tolerar falhas do sistema ou de hardware com o mínimo de impacto para o cliente. Os data centers são construídos em clusters em várias regiões globais. Todos os data centers estão on-line e atendem aos clientes; nenhum data center é “frio”. Em caso de falha, processos automatizados desviam seu tráfego de dados da área afetada. Os aplicativos principais são implantados em uma configuração N+1, de modo que, no caso de uma falha do data center, haja capacidade suficiente para permitir que o tráfego seja balanceado para os locais restantes. A AWS oferece aos clientes a flexibilidade de colocar instâncias e armazenar dados em várias regiões geográficas, bem como em várias zonas de disponibilidade dentro de cada região. Cada zona de disponibilidade é projetada como uma zona de falha independente. Isso significa que as zonas de disponibilidade estão fisicamente separadas dentro de uma região metropolitana típica e estão localizadas em planícies de inundação de menor risco (a categorização específica da zona de inundação varia de acordo com a região). Além da fonte de alimentação ininterrupta (UPS) discreta e das instalações de geração de backup no local, cada uma delas é alimentada por redes diferentes de concessionárias independentes para reduzir ainda mais os pontos únicos de falha. Todas as zonas de disponibilidade são conectadas de forma redundante a vários provedores de trânsito de nível 1. Para obter informações adicionais, consulte o site da AWS Global Infrastructure, disponível em https://aws.amazon.com/about-aws/global-infrastructure/.

Proteção de dados	3.13	Proteger	Implemente uma ferramenta automatizada, como uma ferramenta de Prevenção de perda de dados (DLP) baseada em host para identificar todos os dados confidenciais armazenados, processados ou transmitidos por meio de ativos corporativos, incluindo aqueles localizados no local ou em um provedor de serviços remoto, e atualizar o inventário de dados confidenciais da empresa.		Cliente	Embora no Modelo de Responsabilidade Compartilhada, o controle de acesso aos dados seja responsabilidade do cliente, o serviço AWS Identity and Access Management (IAM) oferece uma maneira simples de listar usuários, grupos, funções e políticas que permitem o acesso aos dados diretamente do console de gerenciamento da AWS. Além disso, nossos clientes podem usar o AWS CloudTrail para monitorar a atividade da conta. O AWS CloudTrail é um serviço que permite a governança, a conformidade, a auditoria operacional e a auditoria de riscos da sua conta da AWS. Com o CloudTrail, você pode registrar, monitorar continuamente e reter a atividade da conta relacionada a ações em toda a sua infraestrutura da AWS. O CloudTrail fornece o histórico de eventos da atividade da sua conta da AWS, incluindo ações realizadas por meio do Console de Gerenciamento da AWS, dos AWS SDKs, das ferramentas de linha de comando e de outros serviços da AWS. Esse histórico de eventos simplifica a análise de segurança, o rastreamento de alterações de recursos e a solução de problemas. Além disso, você pode usar o CloudTrail para detectar atividades incomuns em suas contas da AWS. A segurança e o gerenciamento de usuários usando o IAM são explicados no whitepaper Práticas recomendadas de segurança da AWS, na seção Gerenciar contas da AWS, usuários, grupos e funções do IAM.
Proteção de dados	3.14	Detectar	Registre o acesso a dados confidenciais, incluindo modificação e descarte.		Cliente	Embora no Modelo de Responsabilidade Compartilhada, o controle de acesso aos dados seja responsabilidade do cliente, o serviço AWS Identity and Access Management (IAM) oferece uma maneira simples de listar usuários, grupos, funções e políticas que permitem o acesso aos dados diretamente do console de gerenciamento da AWS. Além disso, nossos clientes podem usar o AWS CloudTrail para monitorar a atividade da conta. O AWS CloudTrail é um serviço que permite a governança, a conformidade, a auditoria operacional e a auditoria de riscos da sua conta da AWS. Com o CloudTrail, você pode registrar, monitorar continuamente e reter a atividade da conta relacionada a ações em toda a sua infraestrutura da AWS. O CloudTrail fornece o histórico de eventos da atividade da sua conta da AWS, incluindo ações realizadas por meio do

						Console de Gerenciamento da AWS, dos AWS SDKs, das ferramentas de linha de comando e de outros serviços da AWS. Esse histórico de eventos simplifica a análise de segurança, o rastreamento de alterações de recursos e a solução de problemas. Além disso, você pode usar o CloudTrail para detectar atividades incomuns em suas contas da AWS. A segurança e o gerenciamento de usuários usando o IAM são explicados no whitepaper Práticas recomendadas de segurança da AWS, na seção Gerenciar contas da AWS, usuários, grupos e funções do IAM.
Configuração segura de ativos e software corporativos	4.1	Proteger	Estabelecer e manter um processo de configuração seguro para ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos não computacionais/IoT; e servidores) e software (sistemas operacionais e aplicativos). Revise e atualize a documentação anualmente ou quando ocorrerem mudanças corporativas significativas que possam afetar essa Proteção.	AWS	Cliente	As definições de configuração do host da AWS são monitoradas para validar a conformidade com os padrões internos de segurança da AWS e enviadas automaticamente para a frota de hosts. O software de gerenciamento de configuração desenvolvido internamente pela AWS é instalado quando um novo hardware é provisionado. Essas ferramentas são executadas em todos os hosts UNIX para validar se eles estão configurados e o software é instalado de maneira padrão com base em classes de host e atualizado regularmente. Somente engenheiros de sistema aprovados e outras partes autorizadas por meio de um serviço de permissões podem fazer login nos servidores centrais de gerenciamento de configuração. As definições de configuração do host são monitoradas para validar a conformidade com os padrões de segurança da AWS e enviadas automaticamente para a frota de hosts. Os clientes da AWS são responsáveis por desenvolver, documentar e manter sob controle de configuração uma configuração de linha de base atual de seus sistemas.
Configuração segura de ativos e software corporativos	4.2	Proteger	Estabeleça e mantenha um processo de configuração seguro para	AWS	Cliente	A rede da AWS consiste em instalações internas de datacenter, servidores, equipamentos de rede e sistemas de software host que estão sob o controle da AWS e são usados para fornecer os serviços. A rede da AWS oferece proteção significativa contra problemas de segurança de rede tradicionais. Por exemplo:

			dispositivos de rede. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças corporativas significativas que possam afetar essa Proteção.			- Ataques distribuídos de negação de serviço (DDoS). - Falsificação de IP - Sniffing de pacotes por outros inquilinos. Além disso, os dispositivos de firewall são configurados para restringir o acesso às redes corporativas e de produção da AWS. As configurações dessas políticas de firewall são mantidas usando um envio automático de um servidor pai a cada 24 horas. Todas as alterações nas políticas de firewall são analisadas e aprovadas pela equipe da AWS. Os clientes da AWS são responsáveis por configurar a segurança de rede em seu ambiente Amazon VPC.
Configuração segura de ativos e software corporativos	4.3	Proteger	Configure o bloqueio automático de sessão em ativos corporativos após um período definido de inatividade. Para sistemas operacionais de uso geral, o período não deve exceder 15 minutos. Para dispositivos móveis de usuário final, o período não deve exceder 2 minutos.	AWS	Cliente	A AWS aplicou uma política de bloqueio de sessão que é aplicada sistematicamente. O bloqueio de sessão é mantido até que os procedimentos de identificação e autenticação sejam realizados. Os clientes da AWS são responsáveis por configurar seus sistemas para encerrar sessões de usuário após condições ou eventos de acionamento ocorrerem de acordo com sua política de controle de acesso.
Configuração segura de ativos e software corporativos	4.4	Proteger	Implemente e gerencie um firewall em servidores, onde houver suporte. Exemplos de implementações incluem um firewall virtual, um firewall do sistema	AWS	Cliente	Os dispositivos de firewall são configurados para restringir o acesso às redes corporativas e de produção da Amazon. As configurações dessas políticas de firewall são mantidas usando um envio automático de um servidor pai a cada 24 horas. Todas as alterações nas políticas de firewall são analisadas e aprovadas pela equipe da AWS. Os clientes da AWS são responsáveis por configurar a segurança de rede em seu ambiente Amazon VPC.

			operacional ou um agente de firewall de terceiros.			
Configuração segura de ativos e software corporativos	4.5	Proteger	Implemente e gerencie um firewall baseado em host ou uma ferramenta de filtragem de portas em dispositivos de usuário final, com uma regra de negação padrão que descarta todo o tráfego, exceto os serviços e portas que são explicitamente permitidos.	AWS	Cliente	Os hosts físicos têm firewalls baseados em host para impedir o acesso não autorizado. O Amazon EC2 fornece uma solução de firewall, conhecida como Security Group; esse firewall de entrada obrigatório é configurado em um modo padrão negar tudo e os clientes do Amazon EC2 devem abrir explicitamente as portas necessárias para permitir o tráfego de entrada
Configuração segura de ativos e software corporativos	4.6	Proteger	Gerencie com segurança os ativos e o software corporativos. Exemplos de implementações incluem o gerenciamento da configuração por meio da infraestrutura como código controlada por versão e o acesso a interfaces administrativas em protocolos de rede seguros, como Secure Shell (SSH) e Hypertext Transfer Protocol	AWS	Cliente	As definições de configuração do host da AWS são monitoradas para validar a conformidade com os padrões internos de segurança da AWS e enviadas automaticamente para a frota de hosts. O software de gerenciamento de configuração desenvolvido internamente pela AWS é instalado quando um novo hardware é provisionado. Essas ferramentas são executadas em todos os hosts UNIX para validar se eles estão configurados e o software é instalado de maneira padrão com base em classes de host e atualizado regularmente. Somente engenheiros de sistema aprovados e outras partes autorizadas por meio de um serviço de permissões podem fazer login nos servidores centrais de gerenciamento de configuração. As definições de configuração do host são monitoradas para validar a conformidade com os padrões de segurança da AWS e enviadas automaticamente para a frota de hosts. A AWS permite que os clientes abram uma sessão segura e criptografada para servidores da AWS usando HTTPS (Transport Layer Security [TLS]). Os clientes da AWS são responsáveis por desenvolver, documentar e manter sob controle de configuração uma configuração de linha de base atual de seus sistemas.

			Secure (HTTPS). Não use protocolos de gerenciamento inseguros, como Telnet (Rede de Teletype) e HTTP, a menos que seja operacionalmente essencial.			
Configuração segura de ativos e software corporativos	4.7	Proteger	Gerencie contas padrão em ativos e software corporativos, como raiz, administrador e outras contas de fornecedor pré-configuradas. Exemplos de implementações podem incluir: desabilitar contas padrão ou torná-las inutilizáveis.	AWS	Cliente	N/A — Os clientes não têm nenhuma responsabilidade na Nuvem AWS pelo inventário de dispositivos e sistemas físicos da AWS. Os clientes são responsáveis apenas por esse controle dos ativos físicos que possuem e operam fora da nuvem (por exemplo, servidores, computadores, equipamentos de rede, dispositivos móveis, dispositivos IoT, periféricos, etc.). Os clientes da AWS são responsáveis por desenvolver, documentar, revisar e atualizar, com uma frequência definida pela organização, um inventário de componentes de software para seus sistemas hospedados na AWS. Os clientes da AWS são responsáveis por verificar se o inventário: 1) reflete com precisão o sistema atual, 2) Inclui todos os componentes dentro do limite de autorização, 3) Está no nível de granularidade considerado necessário para rastreamento e geração de relatórios e 4) Inclui as informações prescritas pela configuração política de gestão que é considerada necessária para alcançar a responsabilidade efetiva dos componentes do sistema de informação.
Configuração segura de ativos e software corporativos	4.8	Proteger	Desinstale ou desative serviços desnecessários em ativos e software corporativos, como um serviço de compartilhamento de arquivos não utilizado, um módulo de aplicativo da Web ou uma função de	AWS	Cliente	As definições de configuração do host da AWS são monitoradas para validar a conformidade com os padrões internos de segurança da AWS e enviadas automaticamente para a frota de hosts. O software de gerenciamento de configuração desenvolvido internamente pela AWS é instalado quando um novo hardware é provisionado. Essas ferramentas são executadas em todos os hosts UNIX para validar se eles estão configurados e o software é instalado de maneira padrão com base em classes de host e atualizado regularmente. Os clientes da AWS são responsáveis por desenvolver, documentar, revisar e atualizar, com uma frequência definida pela organização, um inventário de componentes de software para seus sistemas hospedados na AWS. Os clientes da AWS são responsáveis por verificar se o inventário: 1) reflete com

			serviço.			precisão o sistema atual, 2) Inclui todos os componentes dentro do limite de autorização, 3) Está no nível de granularidade considerado necessário para rastreamento e geração de relatórios e 4) Inclui as informações prescritas pela configuração política de gestão que é considerada necessária para alcançar a responsabilidade efetiva dos componentes do sistema de informação.
Configuração segura de ativos e software corporativos	4.9	Proteger	Configure servidores DNS confiáveis em ativos corporativos. Exemplos de implementações incluem: configurar ativos para usar servidores DNS controlados pela empresa e/ou servidores DNS acessíveis externamente respeitáveis.		Cliente	Os clientes da AWS são responsáveis por todos os serviços do Domain Name System (DNS) que implementam em seus sistemas hospedados na AWS. Dentro desse contexto e de acordo com sua política de proteção de sistemas e comunicações, os clientes da AWS são responsáveis por configurar o DNS para: 1) Fornecer artefatos adicionais de autenticação de origem de dados e verificação de integridade, juntamente com os dados de resolução de nomes autorizados que o sistema retorna em resposta aos consultas externas de resolução de nome/endereço e 2) Fornecer os meios para indicar o status de segurança das zonas filhas e (se o filho oferecer suporte a serviços de resolução segura) para permitir a verificação de uma cadeia de confiança entre os domínios pai e filho, ao operar como parte de um namespace hierárquico distribuído.
Configuração segura de ativos e software corporativos	4.1	Responder	Imponha o bloqueio automático de dispositivos seguindo um limite predeterminado de tentativas de autenticação com falha local em dispositivos portáteis de usuário final, quando suportado. Para laptops, não permita mais de 20 tentativas de autenticação com falha; para tablets e smartphones,	AWS	Cliente	As configurações de senha são gerenciadas em conformidade com a Política de Senhas da AWS. O acesso e a administração da segurança lógica para a Amazon dependem de IDs de usuário, senhas e Kerberos para autenticar usuários em serviços, recursos e dispositivos, bem como para autorizar o nível apropriado de acesso para o usuário. A Segurança da AWS estabeleceu uma política de senhas com configurações e intervalos de expiração necessários. Os clientes da AWS são responsáveis por configurar seus sistemas para impor o bloqueio automático seguindo um limite predeterminado de tentativas de logon com falha.

			não mais do que 10 tentativas de autenticação com falha. Exemplos de implementações incluem o Microsoft® InTune Device Lock e o perfil de configuração da Apple® MaxFailedAttempts.			
Configuração segura de ativos e software corporativos	4.11	Proteger	Limpe remotamente os dados corporativos de dispositivos de usuário final portáteis de propriedade da empresa quando considerado apropriado, como dispositivos perdidos ou roubados, ou quando um indivíduo não oferece mais suporte à empresa.		Cliente	Os clientes mantêm o controle e são responsáveis por seus dados, controles de segurança, exclusão e procedimentos de suporte. Os clientes da AWS são responsáveis por autorizar a conexão de dispositivos móveis e seus recursos de apagamento remoto.
Configuração segura de ativos e software corporativos	4.12	Proteger	Garantir que espaços de trabalho corporativos separados sejam usados em dispositivos móveis de usuário final, onde houver suporte. Exemplos de implementações		Cliente	Os clientes mantêm o controle e são responsáveis por seus dados, controles de segurança, exclusão e procedimentos de suporte. Os clientes da AWS são responsáveis por autorizar a conexão de dispositivos móveis aos seus sistemas antes de permitir a conexão.

			incluem o uso de um perfil de configuração da Apple® ou do Android™ Work Profile para separar aplicativos e dados corporativos de aplicativos e dados pessoais.			
Gerenciamento de contas	5.1	Identificar	Estabelecer e manter um inventário de todas as contas gerenciadas na empresa. O inventário deve incluir contas de usuário e administrador. O inventário, no mínimo, deve conter o nome da pessoa, nome de usuário, datas de início/término e departamento. Valide se todas as contas ativas estão autorizadas, em uma programação recorrente, no mínimo trimestral ou com mais frequência.		Cliente	Embora no Modelo de Responsabilidade Compartilhada, o controle de acesso aos dados seja responsabilidade do cliente, o serviço AWS Identity and Access Management (IAM) oferece uma maneira direta de listar usuários, grupos, funções e políticas que permitem o acesso aos dados diretamente do console de gerenciamento da AWS. Além disso, o IAM pode ser usado para conceder a você acesso federado ao Console de Gerenciamento da AWS e às APIs de serviço da AWS, usando seus sistemas de identidade existentes, como o Microsoft Active Directory. Você pode usar qualquer solução de gerenciamento de identidades que ofereça suporte ao SAML 2.0 ou fique à vontade para usar um de nossos exemplos de federação (SSO do Console AWS ou federação de API). A segurança e o gerenciamento de usuários usando o IAM são explicados no whitepaper Práticas recomendadas de segurança da AWS, na seção Gerenciar contas da AWS, usuários, grupos e funções do IAM.
Gerenciamento de contas	5.2	Proteger	Use senhas exclusivas para todos os ativos corporativos. A implementação das melhores	AWS	Cliente	Embora no Modelo de Responsabilidade Compartilhada, o controle de acesso aos dados seja responsabilidade do cliente, o serviço AWS Identity and Access Management (IAM) oferece uma maneira simples de listar usuários, grupos, funções e políticas que permitem o acesso aos dados diretamente do console de gerenciamento da AWS.

			práticas inclui, no mínimo, uma senha de 8 caracteres para contas que usam MFA e uma senha de 14 caracteres para contas que não usam MFA.			A segurança e o gerenciamento de usuários usando o IAM são explicados no whitepaper Práticas recomendadas de segurança da AWS, na seção Gerenciar contas da AWS, usuários, grupos e funções do IAM. Os clientes mantêm o controle e a responsabilidade de seus dados e ativos de mídia associados. O cliente pode definir sua “Política de senhas” em sua conta da AWS para especificar requisitos de complexidade e períodos de rotação obrigatórios para as senhas dos usuários do IAM. Para obter mais detalhes, consulte Como definir uma política de senha de conta para usuários do IAM, onde você aprenderá a definir uma política de senha na sua conta da AWS para especificar requisitos de complexidade e períodos de rotação obrigatórios para as senhas dos usuários do IAM. A AWS controla o acesso aos sistemas da AWS por meio de autenticação que exige um ID de usuário e senha exclusivos. Os sistemas da AWS não permitem que ações sejam executadas no sistema de informações sem identificação ou autenticação. A AWS aplicou uma política de bloqueio de sessão que é aplicada sistematicamente. O bloqueio de sessão é mantido até que os procedimentos de identificação e autenticação sejam realizados.
Gerenciamento de contas	5.3	Responder	Exclua ou desative todas as contas inativas após um período de 45 dias de inatividade, quando suportado.		Cliente	Embora no Modelo de Responsabilidade Compartilhada, o controle de acesso aos dados seja responsabilidade do cliente, o serviço AWS Identity and Access Management (IAM) oferece uma maneira simples de listar usuários, grupos, funções e políticas que permitem o acesso aos dados diretamente do console de gerenciamento da AWS. Além disso, o IAM pode ser usado para conceder a você acesso federado ao Console de Gerenciamento da AWS e às APIs de serviço da AWS, usando seus sistemas de identidade existentes, como o Microsoft Active Directory. Você pode usar qualquer solução de gerenciamento de identidades que ofereça suporte ao SAML 2.0 ou fique à vontade para usar um de nossos exemplos de federação (SSO do Console AWS ou federação de API). A segurança e o gerenciamento de usuários usando o IAM são explicados no whitepaper Práticas recomendadas de segurança da AWS, na seção

						Gerenciar contas da AWS, usuários, grupos e funções do IAM.
Gerenciamento de contas	5.4	Proteger	Restringir privilégios de administrador a contas de administrador dedicadas em ativos corporativos. Conduza atividades gerais de computação, como navegação na Internet, e-mail e uso do conjunto de produtividade, a partir da conta principal não privilegiada do usuário.		Cliente	Embora no Modelo de Responsabilidade Compartilhada, o controle de acesso aos dados seja responsabilidade do cliente, o serviço AWS Identity and Access Management (IAM) oferece uma maneira simples de listar usuários, grupos, funções e políticas que permitem o acesso aos dados diretamente do console de gerenciamento da AWS. Além disso, o IAM pode ser usado para conceder a você acesso federado ao Console de Gerenciamento da AWS e às APIs de serviço da AWS, usando seus sistemas de identidade existentes, como o Microsoft Active Directory. Você pode usar qualquer solução de gerenciamento de identidades que ofereça suporte ao SAML 2.0 ou fique à vontade para usar um de nossos exemplos de federação (SSO do Console AWS ou federação de API). A segurança e o gerenciamento de usuários usando o IAM são explicados no whitepaper Práticas recomendadas de segurança da AWS, na seção Gerenciar contas da AWS, usuários, grupos e funções do IAM.
Gerenciamento de contas	5.5	Identificar	Estabelecer e manter um inventário de contas de serviço. O inventário, no mínimo, deve conter o proprietário do departamento, a data da revisão e a finalidade. Realize análises de conta de serviço para validar se todas as contas ativas estão autorizadas, em uma programação recorrente, no mínimo trimestral		Cliente	Embora no Modelo de Responsabilidade Compartilhada, o controle de acesso aos dados seja responsabilidade do cliente, o serviço AWS Identity and Access Management (IAM) oferece uma maneira simples de listar usuários, grupos, funções e políticas que permitem o acesso aos dados diretamente do console de gerenciamento da AWS. Além disso, o IAM pode ser usado para conceder a você acesso federado ao Console de Gerenciamento da AWS e às APIs de serviço da AWS, usando seus sistemas de identidade existentes, como o Microsoft Active Directory. Você pode usar qualquer solução de gerenciamento de identidades que ofereça suporte ao SAML 2.0 ou fique à vontade para usar um de nossos exemplos de federação (SSO do Console AWS ou federação de API). A segurança e o gerenciamento de usuários usando o IAM são explicados no whitepaper Práticas recomendadas de segurança da AWS, na seção Gerenciar contas da AWS, usuários, grupos e funções do IAM.

			ou com mais frequência.			
Gerenciamento de contas	5.6	Proteger	Centralize o gerenciamento de contas por meio de um diretório ou serviço de identidade.	AWS	Cliente	Embora no Modelo de Responsabilidade Compartilhada, o controle de acesso aos dados seja responsabilidade do cliente, o serviço AWS Identity and Access Management (IAM) oferece uma maneira simples de listar usuários, grupos, funções e políticas que permitem o acesso aos dados diretamente do console de gerenciamento da AWS. A segurança e o gerenciamento de usuários usando o IAM são explicados no whitepaper Práticas recomendadas de segurança da AWS, na seção Gerenciar contas da AWS, usuários, grupos e funções do IAM. Os clientes mantêm o controle e a responsabilidade de seus dados e ativos de mídia associados. O cliente pode definir sua “Política de senhas” em sua conta da AWS para especificar requisitos de complexidade e períodos de rotação obrigatórios para as senhas dos usuários do IAM. Para obter mais detalhes, consulte Como definir uma política de senha de conta para usuários do IAM, onde você aprenderá a definir uma política de senha na sua conta da AWS para especificar requisitos de complexidade e períodos de rotação obrigatórios para as senhas dos usuários do IAM. A AWS controla o acesso aos sistemas da AWS por meio de autenticação que exige um ID de usuário e senha exclusivos. Os sistemas da AWS não permitem que ações sejam executadas no sistema de informações sem identificação ou autenticação. A AWS aplicou uma política de bloqueio de sessão que é aplicada sistematicamente. O bloqueio de sessão é mantido até que os procedimentos de identificação e autenticação sejam realizados.
Gerenciamento de controle de acesso	6.1	Proteger	Estabeleça e siga um processo, preferencialmente automatizado, para conceder		Cliente	Embora no Modelo de Responsabilidade Compartilhada, o controle de acesso aos dados seja responsabilidade do cliente, o serviço AWS Identity and Access Management (IAM) oferece uma maneira simples de listar usuários, grupos, funções e políticas que permitem o acesso aos dados diretamente do console de gerenciamento da AWS. Além disso, o IAM pode ser usado para

			acesso a ativos corporativos em caso de nova contratação, concessão de direitos ou mudança de função de um usuário.			conceder a você acesso federado ao Console de Gerenciamento da AWS e às APIs de serviço da AWS, usando seus sistemas de identidade existentes, como o Microsoft Active Directory. Você pode usar qualquer solução de gerenciamento de identidades que ofereça suporte ao SAML 2.0 ou fique à vontade para usar um de nossos exemplos de federação (SSO do Console AWS ou federação de API). A segurança e o gerenciamento de usuários usando o IAM são explicados no whitepaper Práticas recomendadas de segurança da AWS, na seção Gerenciar contas da AWS, usuários, grupos e funções do IAM.
Gerenciamento de controle de acesso	6.2	Proteger	Estabelecer e seguir um processo, preferencialmente automatizado, para revogar o acesso a ativos corporativos, desativando contas imediatamente após a rescisão, revogação de direitos ou alteração de função de um usuário. Desativar contas, em vez de excluir contas, pode ser necessário para preservar as trilhas de auditoria.		Cliente	Embora no Modelo de Responsabilidade Compartilhada, o controle de acesso aos dados seja responsabilidade do cliente, o serviço AWS Identity and Access Management (IAM) oferece uma maneira simples de listar usuários, grupos, funções e políticas que permitem o acesso aos dados diretamente do console de gerenciamento da AWS. Além disso, o IAM pode ser usado para conceder a você acesso federado ao Console de Gerenciamento da AWS e às APIs de serviço da AWS, usando seus sistemas de identidade existentes, como o Microsoft Active Directory. Você pode usar qualquer solução de gerenciamento de identidades que ofereça suporte ao SAML 2.0 ou fique à vontade para usar um de nossos exemplos de federação (SSO do Console AWS ou federação de API). A segurança e o gerenciamento de usuários usando o IAM são explicados no whitepaper Práticas recomendadas de segurança da AWS, na seção Gerenciar contas da AWS, usuários, grupos e funções do IAM.
Gerenciamento de controle de acesso	6.3	Proteger	Exigir que todos os aplicativos corporativos ou de terceiros expostos externamente apliquem a MFA,		Cliente	Embora no Modelo de Responsabilidade Compartilhada, o controle de acesso aos dados seja responsabilidade do cliente, o serviço AWS Identity and Access Management (IAM) oferece uma maneira simples de listar usuários, grupos, funções e políticas que permitem o acesso aos dados diretamente do console de gerenciamento da AWS. Além disso, o IAM pode ser usado para conceder a você acesso federado ao Console de Gerenciamento da AWS e

			quando houver suporte. Aplicar a MFA por meio de um serviço de diretório ou provedor de SSO é uma implementação satisfatória deste Safeguard.			às APIs de serviço da AWS, usando seus sistemas de identidade existentes, como o Microsoft Active Directory. Você pode usar qualquer solução de gerenciamento de identidades que ofereça suporte ao SAML 2.0 ou fique à vontade para usar um de nossos exemplos de federação (SSO do Console AWS ou federação de API). A segurança e o gerenciamento de usuários usando o IAM são explicados no whitepaper Práticas recomendadas de segurança da AWS, na seção Gerenciar contas da AWS, usuários, grupos e funções do IAM.
Gerenciamento de controle de acesso	6.4	Proteger	Exigir MFA para acesso remoto à rede.		Cliente	Embora no Modelo de Responsabilidade Compartilhada, o controle de acesso aos dados seja responsabilidade do cliente, o serviço AWS Identity and Access Management (IAM) oferece uma maneira simples de listar usuários, grupos, funções e políticas que permitem o acesso aos dados diretamente do console de gerenciamento da AWS. Além disso, o IAM pode ser usado para conceder a você acesso federado ao Console de Gerenciamento da AWS e às APIs de serviço da AWS, usando seus sistemas de identidade existentes, como o Microsoft Active Directory. Você pode usar qualquer solução de gerenciamento de identidades que ofereça suporte ao SAML 2.0 ou fique à vontade para usar um de nossos exemplos de federação (SSO do Console AWS ou federação de API). A segurança e o gerenciamento de usuários usando o IAM são explicados no whitepaper Práticas recomendadas de segurança da AWS, na seção Gerenciar contas da AWS, usuários, grupos e funções do IAM.
Gerenciamento de controle de acesso	6.5	Proteger	Exigir MFA para todas as contas de acesso administrativo, quando suportadas, em todos os ativos corporativos, sejam gerenciados no local ou por meio de um provedor terceirizado.		Cliente	Embora no Modelo de Responsabilidade Compartilhada, o controle de acesso aos dados seja responsabilidade do cliente, o serviço AWS Identity and Access Management (IAM) oferece uma maneira simples de listar usuários, grupos, funções e políticas que permitem o acesso aos dados diretamente do console de gerenciamento da AWS. Além disso, o IAM pode ser usado para conceder a você acesso federado ao Console de Gerenciamento da AWS e às APIs de serviço da AWS, usando seus sistemas de identidade existentes, como o Microsoft Active Directory. Você pode usar qualquer solução de gerenciamento de identidades que ofereça suporte ao SAML 2.0 ou fique à vontade para usar um de nossos exemplos de federação (SSO do Console AWS ou federação de API). A segurança e o gerenciamento de usuários usando o IAM são explicados no

						whitepaper Práticas recomendadas de segurança da AWS, na seção Gerenciar contas da AWS, usuários, grupos e funções do IAM.
Gerenciamento de controle de acesso	6.6	Identificar	Estabelecer e manter um inventário dos sistemas de autenticação e autorização da empresa, incluindo aqueles hospedados no local ou em um provedor de serviços remoto. Revise e atualize o inventário, no mínimo, anualmente ou com mais frequência.		Cliente	Embora no Modelo de Responsabilidade Compartilhada, o controle de acesso aos dados seja responsabilidade do cliente, o serviço AWS Identity and Access Management (IAM) oferece uma maneira simples de listar usuários, grupos, funções e políticas que permitem o acesso aos dados diretamente do console de gerenciamento da AWS. Além disso, o IAM pode ser usado para conceder a você acesso federado ao Console de Gerenciamento da AWS e às APIs de serviço da AWS, usando seus sistemas de identidade existentes, como o Microsoft Active Directory. Você pode usar qualquer solução de gerenciamento de identidades que ofereça suporte ao SAML 2.0 ou fique à vontade para usar um de nossos exemplos de federação (SSO do Console AWS ou federação de API). A segurança e o gerenciamento de usuários usando o IAM são explicados no whitepaper Práticas recomendadas de segurança da AWS, na seção Gerenciar contas da AWS, usuários, grupos e funções do IAM.
Gerenciamento de controle de acesso	6.7	Proteger	Centralize o controle de acesso para todos os ativos corporativos por meio de um serviço de diretório ou provedor de SSO, quando houver suporte.		Cliente	Embora no Modelo de Responsabilidade Compartilhada, o controle de acesso aos dados seja responsabilidade do cliente, o serviço AWS Identity and Access Management (IAM) oferece uma maneira simples de listar usuários, grupos, funções e políticas que permitem o acesso aos dados diretamente do console de gerenciamento da AWS. Além disso, o IAM pode ser usado para conceder a você acesso federado ao Console de Gerenciamento da AWS e às APIs de serviço da AWS, usando seus sistemas de identidade existentes, como o Microsoft Active Directory. Você pode usar qualquer solução de gerenciamento de identidades que ofereça suporte ao SAML 2.0 ou fique à vontade para usar um de nossos exemplos de federação (SSO do Console AWS ou federação de API). A segurança e o gerenciamento de usuários usando o IAM são explicados no whitepaper Práticas recomendadas de segurança da AWS, na seção Gerenciar contas da AWS, usuários, grupos e funções do IAM.
Gerenciamento de controle de acesso	6.8	Proteger	Definir e manter o controle de acesso baseado em	AWS	Cliente	Embora no Modelo de Responsabilidade Compartilhada, o controle de acesso aos dados seja responsabilidade do cliente, o serviço AWS Identity and Access Management (IAM) oferece uma maneira simples de listar usuários,

			função, determinando e documentando os direitos de acesso necessários para que cada função dentro da empresa realize com êxito suas funções atribuídas. Realize análises de controle de acesso de ativos corporativos para validar se todos os privilégios estão autorizados, em uma programação recorrente, no mínimo, anualmente ou com mais frequência.			grupos, funções e políticas que permitem o acesso aos dados diretamente do console de gerenciamento da AWS. A segurança e o gerenciamento de usuários usando o IAM são explicados no whitepaper Práticas recomendadas de segurança da AWS, na seção Gerenciar contas da AWS, usuários, grupos e funções do IAM. Os clientes mantêm o controle e a responsabilidade de seus dados e ativos de mídia associados. O cliente pode definir sua “Política de senhas” em sua conta da AWS para especificar requisitos de complexidade e períodos de rotação obrigatórios para as senhas dos usuários do IAM. Para obter mais detalhes, consulte Como definir uma política de senha de conta para usuários do IAM, onde você aprenderá a definir uma política de senha na sua conta da AWS para especificar requisitos de complexidade e períodos de rotação obrigatórios para as senhas dos usuários do IAM. A AWS controla o acesso aos sistemas da AWS por meio de autenticação que exige um ID de usuário e senha exclusivos. Os sistemas da AWS não permitem que ações sejam executadas no sistema de informações sem identificação ou autenticação. A AWS aplicou uma política de bloqueio de sessão que é aplicada sistematicamente. O bloqueio de sessão é mantido até que os procedimentos de identificação e autenticação sejam realizados.
Gerenciamento contínuo de vulnerabilidades	7.1	Proteger	Estabelecer e manter um processo documentado de gerenciamento de vulnerabilidades para ativos corporativos. Revise e atualize a documentação anualmente ou quando ocorrerem	AWS	Cliente	A AWS mantém políticas formais que fornecem orientação para a segurança das informações dentro da organização e do ambiente de TI de suporte. A Segurança da AWS estabelece e mantém políticas e procedimentos para delinear padrões de acesso lógico no sistema e nos hosts de infraestrutura da AWS. As políticas também identificam as responsabilidades funcionais pela administração do acesso lógico e da segurança. Quando aplicável, a Segurança da AWS aproveita a estrutura e as políticas do sistema de informações estabelecidas e mantidas pelo Amazon Corporate Information Security. As políticas de segurança de informações corporativas da AWS e da Amazon são revisadas e aprovadas anualmente pela liderança de segurança da AWS e são usadas para apoiar a AWS no cumprimento dos compromissos de serviço assumidos ao cliente.

			mudanças corporativas significativas que possam afetar essa Proteção.			Os clientes da AWS podem realizar avaliações de segurança ou testes de penetração em sua infraestrutura da AWS sem aprovação prévia para os serviços listados. A solicitação de autorização para outros eventos simulados deve ser enviada por meio do formulário Eventos simulados.
Gerenciamento contínuo de vulnerabilidades	7.2	Responder	Estabelecer e manter uma estratégia de remediação baseada em riscos documentada em um processo de remediação, com revisões mensais ou mais frequentes.	AWS	Cliente	A AWS mantém políticas formais que fornecem orientação para a segurança das informações dentro da organização e do ambiente de TI de suporte. A Segurança da AWS estabelece e mantém políticas e procedimentos para delinear padrões de acesso lógico no sistema e nos hosts de infraestrutura da AWS. As políticas também identificam as responsabilidades funcionais pela administração do acesso lógico e da segurança. Quando aplicável, a Segurança da AWS aproveita a estrutura e as políticas do sistema de informações estabelecidas e mantidas pelo Amazon Corporate Information Security. As políticas de segurança de informações corporativas da AWS e da Amazon são revisadas e aprovadas anualmente pela liderança de segurança da AWS e são usadas para apoiar a AWS no cumprimento dos compromissos de serviço assumidos ao cliente. Os clientes da AWS podem realizar avaliações de segurança ou testes de penetração em sua infraestrutura da AWS sem aprovação prévia para os serviços listados. A solicitação de autorização para outros eventos simulados deve ser enviada por meio do formulário Eventos simulados.
Gerenciamento contínuo de vulnerabilidades	7.3	Proteger	Realize atualizações do sistema operacional em ativos corporativos por meio do gerenciamento automatizado de patches mensalmente ou com mais frequência.	AWS	Cliente	A AWS mantém políticas formais que fornecem orientação para a segurança das informações dentro da organização e do ambiente de TI de suporte. A Segurança da AWS estabelece e mantém políticas e procedimentos para delinear padrões de acesso lógico no sistema e nos hosts de infraestrutura da AWS. As políticas também identificam as responsabilidades funcionais pela administração do acesso lógico e da segurança. Quando aplicável, a Segurança da AWS aproveita a estrutura e as políticas do sistema de informações estabelecidas e mantidas pelo Amazon Corporate Information Security. As políticas de segurança de informações corporativas da AWS e da Amazon são revisadas e aprovadas anualmente pela liderança de segurança da AWS e são usadas para apoiar a AWS no cumprimento dos compromissos de serviço assumidos ao cliente. Os clientes da AWS podem realizar avaliações de segurança ou testes de penetração em sua infraestrutura da AWS sem aprovação prévia para os serviços listados. A solicitação de autorização para outros eventos simulados deve ser enviada por meio do formulário Eventos simulados.
	7.4	Proteger		AWS	Cliente	

Gerenciamento contínuo de vulnerabilidades			Execute atualizações de aplicativos em ativos corporativos por meio do gerenciamento automatizado de patches mensalmente ou com mais frequência.			A AWS mantém políticas formais que fornecem orientação para a segurança das informações dentro da organização e do ambiente de TI de suporte. A Segurança da AWS estabelece e mantém políticas e procedimentos para delinear padrões de acesso lógico no sistema e nos hosts de infraestrutura da AWS. As políticas também identificam as responsabilidades funcionais pela administração do acesso lógico e da segurança. Quando aplicável, a Segurança da AWS aproveita a estrutura e as políticas do sistema de informações estabelecidas e mantidas pelo Amazon Corporate Information Security. As políticas de segurança de informações corporativas da AWS e da Amazon são revisadas e aprovadas anualmente pela liderança de segurança da AWS e são usadas para apoiar a AWS no cumprimento dos compromissos de serviço assumidos ao cliente. Os clientes da AWS podem realizar avaliações de segurança ou testes de penetração em sua infraestrutura da AWS sem aprovação prévia para os serviços listados. A solicitação de autorização para outros eventos simulados deve ser enviada por meio do formulário Eventos simulados.
Gerenciamento contínuo de vulnerabilidades	7.5	Identificar	Realize varreduras automatizadas de vulnerabilidades de ativos corporativos internos trimestralmente ou com mais frequência. Conduza varreduras autenticadas e não autenticadas, usando uma ferramenta de verificação de vulnerabilidades compatível com SCAPE.	AWS	Cliente	A AWS mantém políticas formais que fornecem orientação para a segurança das informações dentro da organização e do ambiente de TI de suporte. A Segurança da AWS estabelece e mantém políticas e procedimentos para delinear padrões de acesso lógico no sistema e nos hosts de infraestrutura da AWS. As políticas também identificam as responsabilidades funcionais pela administração do acesso lógico e da segurança. Quando aplicável, a Segurança da AWS aproveita a estrutura e as políticas do sistema de informações estabelecidas e mantidas pelo Amazon Corporate Information Security. As políticas de segurança de informações corporativas da AWS e da Amazon são revisadas e aprovadas anualmente pela liderança de segurança da AWS e são usadas para apoiar a AWS no cumprimento dos compromissos de serviço assumidos ao cliente. Os clientes da AWS podem realizar avaliações de segurança ou testes de penetração em sua infraestrutura da AWS sem aprovação prévia para os serviços listados. A solicitação de autorização para outros eventos simulados deve ser enviada por meio do formulário Eventos simulados.
Gerenciamento contínuo de vulnerabilidades	7.6	Identificar	Execute varreduras automatizadas de vulnerabilidades	AWS	Cliente	A AWS mantém políticas formais que fornecem orientação para a segurança das informações dentro da organização e do ambiente de TI de suporte. A Segurança da AWS estabelece e mantém políticas e procedimentos para delinear padrões de acesso lógico no sistema e nos hosts de infraestrutura da

			de ativos corporativos expostos externamente usando uma ferramenta de verificação de vulnerabilidades compatível com o SCAPE. Realize varreduras mensalmente ou com mais frequência.			AWS. As políticas também identificam as responsabilidades funcionais pela administração do acesso lógico e da segurança. Quando aplicável, a Segurança da AWS aproveita a estrutura e as políticas do sistema de informações estabelecidas e mantidas pelo Amazon Corporate Information Security. As políticas de segurança de informações corporativas da AWS e da Amazon são revisadas e aprovadas anualmente pela liderança de segurança da AWS e são usadas para apoiar a AWS no cumprimento dos compromissos de serviço assumidos ao cliente. Os clientes da AWS podem realizar avaliações de segurança ou testes de penetração em sua infraestrutura da AWS sem aprovação prévia para os serviços listados. A solicitação de autorização para outros eventos simulados deve ser enviada por meio do formulário Eventos simulados.
Gerenciamento contínuo de vulnerabilidades	7.7	Responder	Corrija as vulnerabilidades detectadas no software por meio de processos e ferramentas mensalmente ou com mais frequência, com base no processo de correção.	AWS	Cliente	A AWS mantém políticas formais que fornecem orientação para a segurança das informações dentro da organização e do ambiente de TI de suporte. A Segurança da AWS estabelece e mantém políticas e procedimentos para delinear padrões de acesso lógico no sistema e nos hosts de infraestrutura da AWS. As políticas também identificam as responsabilidades funcionais pela administração do acesso lógico e da segurança. Quando aplicável, a Segurança da AWS aproveita a estrutura e as políticas do sistema de informações estabelecidas e mantidas pelo Amazon Corporate Information Security. As políticas de segurança de informações corporativas da AWS e da Amazon são revisadas e aprovadas anualmente pela liderança de segurança da AWS e são usadas para apoiar a AWS no cumprimento dos compromissos de serviço assumidos ao cliente. Os clientes da AWS podem realizar avaliações de segurança ou testes de penetração em sua infraestrutura da AWS sem aprovação prévia para os serviços listados. A solicitação de autorização para outros eventos simulados deve ser enviada por meio do formulário Eventos simulados.
Gerenciamento de registros de auditoria	8.1	Proteger	Estabelecer e manter um processo de gerenciamento de registros de auditoria que defina os requisitos de registro da		Customer	Embora no Modelo de Responsabilidade Compartilhada, o controle de acesso aos dados seja responsabilidade do cliente, o serviço AWS Identity and Access Management (IAM) oferece uma maneira simples de listar usuários, grupos, funções e políticas que permitem o acesso aos dados diretamente do console de gerenciamento da AWS. Além disso, nossos clientes podem usar o AWS CloudTrail para monitorar a atividade da conta. O AWS CloudTrail é um serviço que permite a

			empresa. No mínimo, trate da coleta, revisão e retenção de registros de auditoria para ativos corporativos. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças corporativas significativas que possam afetar essa Proteção.			governança, a conformidade, a auditoria operacional e a auditoria de riscos da sua conta da AWS. Com o CloudTrail, você pode registrar, monitorar continuamente e reter a atividade da conta relacionada a ações em toda a sua infraestrutura da AWS. O CloudTrail fornece o histórico de eventos da atividade da sua conta da AWS, incluindo ações realizadas por meio do Console de Gerenciamento da AWS, dos AWS SDKs, das ferramentas de linha de comando e de outros serviços da AWS. Esse histórico de eventos simplifica a análise de segurança, o rastreamento de alterações de recursos e a solução de problemas. Além disso, você pode usar o CloudTrail para detectar atividades incomuns em suas contas da AWS. A segurança e o gerenciamento de usuários usando o IAM são explicados no whitepaper Práticas recomendadas de segurança da AWS, na seção Gerenciar contas da AWS, usuários, grupos e funções do IAM.
Gerenciamento de registros de auditoria	8.2	Detectar	Colete registros de auditoria. Certifique-se de que o registro, de acordo com o processo de gerenciamento de log de auditoria da empresa, tenha sido habilitado em todos os ativos da empresa.	AWS	Cliente	As atividades do sistema são registradas, mantidas por um período definido e protegidas contra modificações não autorizadas.
Gerenciamento de registros de auditoria	8.3	Proteger	Garantir que os destinos de registro mantenham o armazenamento adequado para cumprir o processo de gerenciamento de registros de auditoria da empresa.	AWS	Cliente	As atividades do sistema são registradas, mantidas por um período definido e protegidas contra modificações não autorizadas.

Gerenciamento de registros de auditoria	8.4	Proteger	Padronize a sincronização de tempo. Configure pelo menos duas fontes de tempo sincronizadas em todos os ativos da empresa, onde houver suporte.	AWS	Cliente	Os sistemas de informações da AWS usam relógios de sistema internos sincronizados por meio do Network Time Protocol (NTP) ou de uma fonte comparável para gerar carimbos de data/hora para registros de auditoria. Os testes de terceiros dos carimbos de data/hora da AWS validam que a hora do sistema está configurada para sincronizar automaticamente com fontes de tempo aprovadas do estrato 1. A AWS oferece aos clientes propriedade e controle sobre os relógios do sistema em seu ambiente operacional hospedado. Os clientes da AWS são responsáveis por configurar a sincronização de horário com servidores de horário, conforme exigido por sua organização.
Gerenciamento de registros de auditoria	8.5	Detectar	Configure o log de auditoria detalhado para ativos corporativos que contêm dados confidenciais. Inclua origem do evento, data, nome de usuário, carimbo de data/hora, endereços de origem, endereços de destino e outros elementos úteis que possam auxiliar em uma investigação forense.	AWS	Cliente	A AWS implanta dispositivos de monitoramento em todo o ambiente para coletar informações críticas sobre tentativas de invasão não autorizadas, abuso de uso e uso da largura de banda da rede e do aplicativo. Os dispositivos de monitoramento são colocados no ambiente da AWS para detectar e monitorar: - Ataques de varredura de portas - Uso (CPU, processos, utilização de disco, taxas de swap e erros na perda gerada por software) - Métricas de desempenho de aplicativos - Tentativas de conexão não autorizada A AWS fornece alertas quase em tempo real quando as ferramentas de monitoramento da AWS mostram indicações de comprometimento ou possível comprometimento, com base em mecanismos de alarme de limite determinados pelas equipes de serviço e segurança da AWS. O acesso externo aos dados armazenados no Amazon S3 é registrado. Os registros são retidos por pelo menos 90 dias e incluem informações relevantes da solicitação de acesso, como o endereço IP, o objeto e a operação do acessador de dados. Todas as solicitações para o KMS são registradas e estão disponíveis no bucket do AWS CloudTrail da conta da AWS no Amazon S3. As solicitações registradas fornecem informações sobre quem fez a solicitação e sob qual

						CMK e também descreverão informações sobre o recurso da AWS que foi protegido por meio do uso da CMK. Esses eventos de log ficam visíveis para o cliente depois de ativar o AWS CloudTrail em sua conta. Os clientes da AWS são responsáveis por definir, documentar e implementar soluções de auditoria e monitoramento para seus sistemas. Isso inclui definir os eventos a serem auditados por cada componente do sistema em seu sistema, implementar a auditoria para capturar informações para suporte após as investigações de fatos e determinar uma solução para análise de auditoria, redução e geração de relatórios.
Gerenciamento de registros de auditoria	8.6	Detectar	Colete registros de auditoria de consulta de DNS em ativos corporativos, quando apropriado e suportado.	AWS	Cliente	A AWS implanta dispositivos de monitoramento em todo o ambiente para coletar informações críticas sobre tentativas de invasão não autorizadas, abuso de uso e uso da largura de banda da rede e do aplicativo. Os dispositivos de monitoramento são colocados no ambiente da AWS para detectar e monitorar: - Ataques de varredura de portas - Uso (CPU, processos, utilização de disco, taxas de swap e erros na perda gerada por software) - Métricas de desempenho de aplicativos - Tentativas de conexão não autorizada A AWS fornece alertas quase em tempo real quando as ferramentas de monitoramento da AWS mostram indicações de comprometimento ou possível comprometimento, com base em mecanismos de alarme de limite determinados pelas equipes de serviço e segurança da AWS. O acesso externo aos dados armazenados no Amazon S3 é registrado. Os registros são retidos por pelo menos 90 dias e incluem informações relevantes da solicitação de acesso, como o endereço IP, o objeto e a operação do acessador de dados. Todas as solicitações para o KMS são registradas e estão disponíveis no bucket do AWS CloudTrail da conta da AWS no Amazon S3. As solicitações registradas fornecem informações sobre quem fez a solicitação e sob qual CMK e também descreverão informações sobre o recurso da AWS que foi

						protegido por meio do uso da CMK. Esses eventos de log ficam visíveis para o cliente depois de ativar o AWS CloudTrail em sua conta. Os clientes da AWS são responsáveis por definir, documentar e implementar soluções de auditoria e monitoramento para seus sistemas. Isso inclui definir os eventos a serem auditados por cada componente do sistema em seu sistema, implementar a auditoria para capturar informações para suporte após as investigações de fatos e determinar uma solução para análise de auditoria, redução e geração de relatórios.
Gerenciamento de registros de auditoria	8.7	Detectar	Colete registros de auditoria de solicitação de URL em ativos corporativos, quando apropriado e suportado.	AWS	Cliente	A AWS implanta dispositivos de monitoramento em todo o ambiente para coletar informações críticas sobre tentativas de invasão não autorizadas, abuso de uso e uso da largura de banda da rede e do aplicativo. Os dispositivos de monitoramento são colocados no ambiente da AWS para detectar e monitorar: - Ataques de varredura de portas - Uso (CPU, processos, utilização de disco, taxas de swap e erros na perda gerada por software) - Métricas de desempenho de aplicativos - Tentativas de conexão não autorizada A AWS fornece alertas quase em tempo real quando as ferramentas de monitoramento da AWS mostram indicações de comprometimento ou possível comprometimento, com base em mecanismos de alarme de limite determinados pelas equipes de serviço e segurança da AWS. O acesso externo aos dados armazenados no Amazon S3 é registrado. Os registros são retidos por pelo menos 90 dias e incluem informações relevantes da solicitação de acesso, como o endereço IP, o objeto e a operação do acessador de dados. Todas as solicitações para o KMS são registradas e estão disponíveis no bucket do AWS CloudTrail da conta da AWS no Amazon S3. As solicitações registradas fornecem informações sobre quem fez a solicitação e sob qual CMK e também descreverão informações sobre o recurso da AWS que foi protegido por meio do uso da CMK. Esses eventos de log ficam visíveis para

						o cliente depois de ativar o AWS CloudTrail em sua conta. Os clientes da AWS são responsáveis por definir, documentar e implementar soluções de auditoria e monitoramento para seus sistemas. Isso inclui definir os eventos a serem auditados por cada componente do sistema em seu sistema, implementar a auditoria para capturar informações para suporte após as investigações de fatos e determinar uma solução para análise de auditoria, redução e geração de relatórios.
Gerenciamento de registros de auditoria	8.8	Detectar	Colete registros de auditoria de linha de comando. Exemplos de implementações incluem a coleta de logs de auditoria do PowerShell®, BASH™ e terminais administrativos remotos.	AWS	Cliente	A AWS implanta dispositivos de monitoramento em todo o ambiente para coletar informações críticas sobre tentativas de invasão não autorizadas, abuso de uso e uso da largura de banda da rede e do aplicativo. Os dispositivos de monitoramento são colocados no ambiente da AWS para detectar e monitorar: - Ataques de varredura de portas - Uso (CPU, processos, utilização de disco, taxas de swap e erros na perda gerada por software) - Métricas de desempenho de aplicativos - Tentativas de conexão não autorizada A AWS fornece alertas quase em tempo real quando as ferramentas de monitoramento da AWS mostram indicações de comprometimento ou possível comprometimento, com base em mecanismos de alarme de limite determinados pelas equipes de serviço e segurança da AWS. O acesso externo aos dados armazenados no Amazon S3 é registrado. Os registros são retidos por pelo menos 90 dias e incluem informações relevantes da solicitação de acesso, como o endereço IP, o objeto e a operação do acessador de dados. Todas as solicitações para o KMS são registradas e estão disponíveis no bucket do AWS CloudTrail da conta da AWS no Amazon S3. As solicitações registradas fornecem informações sobre quem fez a solicitação e sob qual CMK e também descreverão informações sobre o recurso da AWS que foi protegido por meio do uso da CMK. Esses eventos de log ficam visíveis para o cliente depois de ativar o AWS CloudTrail em sua conta.

						Os clientes da AWS são responsáveis por definir, documentar e implementar soluções de auditoria e monitoramento para seus sistemas. Isso inclui definir os eventos a serem auditados por cada componente do sistema em seu sistema, implementar a auditoria para capturar informações para suporte após as investigações de fatos e determinar uma solução para análise de auditoria, redução e geração de relatórios.
Gerenciamento de registros de auditoria	8.9	Detectar	Centralize, na medida do possível, a coleta e a retenção de registros de auditoria em todos os ativos corporativos.	AWS	Cliente	A AWS implanta dispositivos de monitoramento em todo o ambiente para coletar informações críticas sobre tentativas de invasão não autorizadas, abuso de uso e uso da largura de banda da rede e do aplicativo. Os dispositivos de monitoramento são colocados no ambiente da AWS para detectar e monitorar: - Ataques de varredura de portas - Uso (CPU, processos, utilização de disco, taxas de swap e erros na perda gerada por software) - Métricas de desempenho de aplicativos - Tentativas de conexão não autorizada A AWS fornece alertas quase em tempo real quando as ferramentas de monitoramento da AWS mostram indicações de comprometimento ou possível comprometimento, com base em mecanismos de alarme de limite determinados pelas equipes de serviço e segurança da AWS. O acesso externo aos dados armazenados no Amazon S3 é registrado. Os registros são retidos por pelo menos 90 dias e incluem informações relevantes da solicitação de acesso, como o endereço IP, o objeto e a operação do acessador de dados. Todas as solicitações para o KMS são registradas e estão disponíveis no bucket do AWS CloudTrail da conta da AWS no Amazon S3. As solicitações registradas fornecem informações sobre quem fez a solicitação e sob qual CMK e também descreverão informações sobre o recurso da AWS que foi protegido por meio do uso da CMK. Esses eventos de log ficam visíveis para o cliente depois de ativar o AWS CloudTrail em sua conta.

						Os clientes da AWS são responsáveis por definir, documentar e implementar soluções de auditoria e monitoramento para seus sistemas. Isso inclui definir os eventos a serem auditados por cada componente do sistema em seu sistema, implementar a auditoria para capturar informações para suporte após as investigações de fatos e determinar uma solução para análise de auditoria, redução e geração de relatórios.
Gerenciamento de registros de auditoria	8.1	Proteger	Mantenha os registros de auditoria em todos os ativos da empresa por um período mínimo de 90 dias.	AWS	Cliente	A AWS implanta dispositivos de monitoramento em todo o ambiente para coletar informações críticas sobre tentativas de invasão não autorizadas, abuso de uso e uso da largura de banda da rede e do aplicativo. Os dispositivos de monitoramento são colocados no ambiente da AWS para detectar e monitorar: - Ataques de varredura de portas - Uso (CPU, processos, utilização de disco, taxas de swap e erros na perda gerada por software) - Métricas de desempenho de aplicativos - Tentativas de conexão não autorizada A AWS fornece alertas quase em tempo real quando as ferramentas de monitoramento da AWS mostram indicações de comprometimento ou possível comprometimento, com base em mecanismos de alarme de limite determinados pelas equipes de serviço e segurança da AWS. O acesso externo aos dados armazenados no Amazon S3 é registrado. Os registros são retidos por pelo menos 90 dias e incluem informações relevantes da solicitação de acesso, como o endereço IP, o objeto e a operação do acessador de dados. Todas as solicitações para o KMS são registradas e estão disponíveis no bucket do AWS CloudTrail da conta da AWS no Amazon S3. As solicitações registradas fornecem informações sobre quem fez a solicitação e sob qual CMK e também descreverão informações sobre o recurso da AWS que foi protegido por meio do uso da CMK. Esses eventos de log ficam visíveis para o cliente depois de ativar o AWS CloudTrail em sua conta.

						Os clientes da AWS são responsáveis por definir, documentar e implementar soluções de auditoria e monitoramento para seus sistemas. Isso inclui definir os eventos a serem auditados por cada componente do sistema em seu sistema, implementar a auditoria para capturar informações para suporte após as investigações de fatos e determinar uma solução para análise de auditoria, redução e geração de relatórios.
Gerenciamento de registros de auditoria	8.11	Detectar	Realize análises dos registros de auditoria para detectar anomalias ou eventos anormais que possam indicar uma possível ameaça. Realize revisões semanalmente ou com mais frequência.	AWS	Cliente	A AWS implanta dispositivos de monitoramento em todo o ambiente para coletar informações críticas sobre tentativas de invasão não autorizadas, abuso de uso e uso da largura de banda da rede e do aplicativo. Os dispositivos de monitoramento são colocados no ambiente da AWS para detectar e monitorar: - Ataques de varredura de portas - Uso (CPU, processos, utilização de disco, taxas de swap e erros na perda gerada por software) - Métricas de desempenho de aplicativos - Tentativas de conexão não autorizada A AWS fornece alertas quase em tempo real quando as ferramentas de monitoramento da AWS mostram indicações de comprometimento ou possível comprometimento, com base em mecanismos de alarme de limite determinados pelas equipes de serviço e segurança da AWS. Os clientes da AWS são responsáveis por definir, documentar e implementar soluções de auditoria e monitoramento para seus sistemas. Isso inclui definir os eventos a serem auditados por cada componente do sistema em seu sistema, implementar a auditoria para capturar informações para suporte após as investigações de fatos e determinar uma solução para análise de auditoria, redução e geração de relatórios.
Gerenciamento de registros de auditoria	8.12	Detectar	Colete registros do provedor de serviços, quando houver suporte. Exemplos de implementações incluem a coleta de eventos de autenticação e autorização, eventos de criação e descarte de dados e eventos	AWS	Cliente	A AWS implanta dispositivos de monitoramento em todo o ambiente para coletar informações críticas sobre tentativas de invasão não autorizadas, abuso de uso e uso da largura de banda da rede e do aplicativo. Os dispositivos de monitoramento são colocados no ambiente da AWS para detectar e monitorar: - Ataques de varredura de portas - Uso (CPU, processos, utilização de disco, taxas de swap e erros na perda gerada por software) - Métricas de desempenho de aplicativos

			de gerenciamento de usuários.			- Tentativas de conexão não autorizada A AWS fornece alertas quase em tempo real quando as ferramentas de monitoramento da AWS mostram indicações de comprometimento ou possível comprometimento, com base em mecanismos de alarme de limite determinados pelas equipes de serviço e segurança da AWS. O acesso externo aos dados armazenados no Amazon S3 é registrado. Os registros são retidos por pelo menos 90 dias e incluem informações relevantes da solicitação de acesso, como o endereço IP, o objeto e a operação do acessador de dados. Todas as solicitações para o KMS são registradas e estão disponíveis no bucket do AWS CloudTrail da conta da AWS no Amazon S3. As solicitações registradas fornecem informações sobre quem fez a solicitação e sob qual CMK e também descreverão informações sobre o recurso da AWS que foi protegido por meio do uso da CMK. Esses eventos de log ficam visíveis para o cliente depois de ativar o AWS CloudTrail em sua conta. Os clientes da AWS são responsáveis por definir, documentar e implementar soluções de auditoria e monitoramento para seus sistemas. Isso inclui definir os eventos a serem auditados por cada componente do sistema em seu sistema, implementar a auditoria para capturar informações para suporte após as investigações de fatos e determinar uma solução para análise de auditoria, redução e geração de relatórios.
Proteções de e-mail e navegador da Web	9.1	Proteger	Certifique-se de que apenas navegadores e clientes de e-mail com suporte total tenham permissão para executar na empresa, usando apenas a versão mais recente dos navegadores e clientes de e-mail fornecidos pelo fornecedor.	AWS	Cliente	Os usuários gerais não têm direitos para instalar o software. Antes da instalação, todos os softwares estão sujeitos a revisões na lista branca. O processo de whitelisting ocorre como parte de uma revisão mensal com os proprietários de serviços da AWS para garantir que somente o software na lista de permissões seja implantado. Os clientes da AWS são responsáveis por estabelecer, aplicar e monitorar políticas de instalação de software que regem a instalação de software pelos usuários com base em métodos definidos pela organização e frequência de monitoramento.

Proteções de e-mail e navegador da Web	9.2	Proteger	Use os serviços de filtragem de DNS em todos os ativos corporativos para bloquear o acesso a domínios mal-intencionados conhecidos.	AWS	Cliente	Os ativos da Amazon (por exemplo, laptops) são configurados com software antivírus que inclui filtragem de e-mail e detecção de malware. Os clientes da AWS são responsáveis pela implementação e configuração de mecanismos de monitoramento e proteção baseados em host, incluindo software antivírus e antimalware, ferramentas de verificação de integridade, detecção/prevenção de intrusão baseada em host e proteção contra spam.
Proteções de e-mail e navegador da Web	9.3	Proteger	Imponha e atualize filtros de URL baseados em rede para impedir que um ativo corporativo se conecte a sites potencialmente mal-intencionados ou não aprovados. Exemplos de implementações incluem filtragem baseada em categoria, filtragem baseada em reputação ou por meio do uso de listas de bloqueio. Aplique filtros para todos os ativos corporativos.	AWS	Cliente	Os ativos da Amazon (por exemplo, laptops) são configurados com software antivírus que inclui filtragem de e-mail e detecção de malware. Os clientes da AWS são responsáveis pela implementação e configuração de mecanismos de monitoramento e proteção baseados em host, incluindo software antivírus e antimalware, ferramentas de verificação de integridade, detecção/prevenção de intrusão baseada em host e proteção contra spam.
Proteções de e-mail e navegador da Web	9.4	Proteger	Restrinja, seja por meio da desinstalação ou desativação, qualquer navegador não autorizado ou desnecessário ou plugins de cliente	AWS	Cliente	Os usuários gerais não têm direitos para instalar o software. Antes da instalação, todos os softwares estão sujeitos a revisões na lista branca. O processo de whitelisting ocorre como parte de uma revisão mensal com os proprietários de serviços da AWS para garantir que somente o software na lista de permissões seja implantado. Os clientes da AWS são responsáveis por estabelecer, aplicar e monitorar políticas de instalação de software que regem a instalação de software pelos usuários com base em métodos definidos pela organização e frequência de monitoramento.

			de e-mail, extensões e aplicativos complementares.			
Proteções de e-mail e navegador da Web	9.5	Proteger	Para diminuir a chance de e-mails falsificados ou modificados de domínios válidos, implemente a política e a verificação do DMARC, começando com a implementação dos padrões Sender Policy Framework (SPF) e DomainKeys Identified Mail (DKIM).	AWS	Cliente	Os ativos da Amazon (por exemplo, laptops) são configurados com software antivírus que inclui filtragem de e-mail e detecção de malware. Os clientes da AWS são responsáveis pela implementação e configuração de mecanismos de monitoramento e proteção baseados em host, incluindo software antivírus e antimalware, ferramentas de verificação de integridade, detecção/prevenção de intrusão baseada em host e proteção contra spam.
Proteções de e-mail e navegador da Web	9.6	Proteger	Bloqueie tipos de arquivos desnecessários que tentam entrar no gateway de e-mail da empresa.	AWS	Cliente	Os ativos da Amazon (por exemplo, laptops) são configurados com software antivírus que inclui filtragem de e-mail e detecção de malware. Os clientes da AWS são responsáveis pela implementação e configuração de mecanismos de monitoramento e proteção baseados em host, incluindo software antivírus e antimalware, ferramentas de verificação de integridade, detecção/prevenção de intrusão baseada em host e proteção contra spam.
Proteções de e-mail e navegador da Web	9.7	Proteger	Implante e mantenha proteções antimalware do servidor de e-mail, como verificação de anexos e/ou sandbox.	AWS	Cliente	Os ativos da Amazon (por exemplo, laptops) são configurados com software antivírus que inclui filtragem de e-mail e detecção de malware. Os clientes da AWS são responsáveis pela implementação e configuração de mecanismos de monitoramento e proteção baseados em host, incluindo software antivírus e antimalware, ferramentas de verificação de integridade, detecção/prevenção de intrusão baseada em host e proteção contra spam.
Defesas contra	10.1	Proteger	Implante e mantenha software	AWS	Cliente	Os ativos da Amazon (por exemplo, laptops) são configurados com software antivírus que inclui filtragem de e-mail e detecção de malware.

malware			antimalware em todos os ativos corporativos.			Os clientes da AWS são responsáveis pela implementação e configuração de mecanismos de monitoramento e proteção baseados em host, incluindo software antivírus e antimalware, ferramentas de verificação de integridade, detecção/prevenção de intrusão baseada em host e proteção contra spam.
Defesas contra malware	10.2	Proteger	Configure atualizações automáticas para arquivos de assinatura antimalware em todos os ativos corporativos.	AWS	Cliente	Os ativos da Amazon (por exemplo, laptops) são configurados com software antivírus que inclui filtragem de e-mail e detecção de malware. Os clientes da AWS são responsáveis pela implementação e configuração de mecanismos de monitoramento e proteção baseados em host, incluindo software antivírus e antimalware, ferramentas de verificação de integridade, detecção/prevenção de intrusão baseada em host e proteção contra spam.
Defesas contra malware	10.3	Proteger	Desative a funcionalidade de execução automática e execução automática para mídia removível.	AWS	Cliente	Os ativos da Amazon (por exemplo, laptops) são configurados com software antivírus que inclui filtragem de e-mail e detecção de malware. Os clientes da AWS são responsáveis pela implementação e configuração de mecanismos de monitoramento e proteção baseados em host, incluindo software antivírus e antimalware, ferramentas de verificação de integridade, detecção/prevenção de intrusão baseada em host e proteção contra spam.
Defesas contra malware	10.4	Detectar	Configure o software antimalware para verificar automaticamente a mídia removível.	AWS	Cliente	Os ativos da Amazon (por exemplo, laptops) são configurados com software antivírus que inclui filtragem de e-mail e detecção de malware. Os clientes da AWS são responsáveis pela implementação e configuração de mecanismos de monitoramento e proteção baseados em host, incluindo software antivírus e antimalware, ferramentas de verificação de integridade, detecção/prevenção de intrusão baseada em host e proteção contra spam.
Defesas contra malware	10.5	Proteger	Ative recursos antiexploração em ativos e software corporativos, sempre que possível, como o Microsoft® Data Execution Prevention (DEP), o Windows® Defender Exploit Guard (WDEG) ou o	AWS	Cliente	Os ativos da Amazon (por exemplo, laptops) são configurados com software antivírus que inclui filtragem de e-mail e detecção de malware. Os clientes da AWS são responsáveis pela implementação e configuração de mecanismos de monitoramento e proteção baseados em host, incluindo software antivírus e antimalware, ferramentas de verificação de integridade, detecção/prevenção de intrusão baseada em host e proteção contra spam.

			Apple® System Integrity Protection (SIP) e Gatekeeper™.			
Defesas contra malware	10.6	Proteger	Gerencie centralmente o software antimalware.	AWS	Cliente	Os ativos da Amazon (por exemplo, laptops) são configurados com software antivírus que inclui filtragem de e-mail e detecção de malware. Os clientes da AWS são responsáveis pela implementação e configuração de mecanismos de monitoramento e proteção baseados em host, incluindo software antivírus e antimalware, ferramentas de verificação de integridade, detecção/prevenção de intrusão baseada em host e proteção contra spam.
Defesas contra malware	10.7	Detectar	Use um software antimalware baseado em comportamento.	AWS	Cliente	Os ativos da Amazon (por exemplo, laptops) são configurados com software antivírus que inclui filtragem de e-mail e detecção de malware. Os clientes da AWS são responsáveis pela implementação e configuração de mecanismos de monitoramento e proteção baseados em host, incluindo software antivírus e antimalware, ferramentas de verificação de integridade, detecção/prevenção de intrusão baseada em host e proteção contra spam.
Recuperação de dados	11.1	Recuperar	Estabeleça e mantenha um processo de recuperação de dados. No processo, trate do escopo das atividades de recuperação de dados, da priorização da recuperação e da segurança dos dados de backup. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças corporativas significativas que possam afetar		Customer	A AWS oferece aos clientes ferramentas para configurar e usar adequadamente as ofertas de serviços da AWS para manter a segurança, a proteção e o backup adequados dos dados dos clientes. A AWS permite que os clientes realizem seus próprios backups usando serviços como o AWS Backup, que é um serviço de backup totalmente gerenciado que simplifica a centralização e a automatização do backup de dados nos serviços da AWS na Cloud e no local usando o AWS Storage Gateway. Usando o AWS Backup, os clientes podem configurar centralmente políticas de backup e monitorar atividades de backup para recursos da AWS, como volumes do Amazon EBS, bancos de dados do Amazon RDS, tabelas do Amazon DynamoDB, sistemas de arquivos do Amazon EFS e volumes do AWS Storage Gateway. O AWS Backup automatiza e consolida tarefas de backup executadas anteriormente serviço por serviço, eliminando a necessidade de criar scripts personalizados e processos manuais. Com apenas alguns cliques no console do AWS Backup, os clientes podem criar políticas de backup que automatizam as agendas de backup e o gerenciamento de retenção. O AWS Backup oferece uma solução de backup totalmente gerenciada e baseada em políticas, simplificando o gerenciamento de backup, ajudando que você atenda aos requisitos de conformidade de backup normativos e de negócios.

			essa Proteção.			Para obter mais informações, consulte o whitepaper sobre abordagens de backup e recuperação usando a AWS, disponível em https://d0.awsstatic.com/whitepapers/Backup_and_Recovery_Approaches_Using_AWS.pdf
Recuperação de dados	11.2	Recuperar	Realize backups automatizados de ativos corporativos dentro do escopo. Execute backups semanalmente, ou com mais frequência, com base na sensibilidade dos dados.		Customer	A AWS oferece aos clientes a capacidade de configurar e usar adequadamente as ofertas de serviços da AWS para manter a segurança, a proteção e o backup adequados dos dados dos clientes. A AWS permite que os clientes realizem seus próprios backups usando serviços como o AWS Backup, que é um serviço de backup totalmente gerenciado que simplifica a centralização e a automatização do backup de dados nos serviços da AWS na Cloud e no local usando o AWS Storage Gateway. Usando o AWS Backup, os clientes podem configurar centralmente políticas de backup e monitorar atividades de backup para recursos da AWS, como volumes do Amazon EBS, bancos de dados do Amazon RDS, tabelas do Amazon DynamoDB, sistemas de arquivos do Amazon EFS e volumes do AWS Storage Gateway. O AWS Backup automatiza e consolida tarefas de backup executadas anteriormente serviço por serviço, eliminando a necessidade de criar scripts personalizados e processos manuais. Com apenas alguns cliques no console do AWS Backup, os clientes podem criar políticas de backup que automatizam as agendas de backup e o gerenciamento de retenção. O AWS Backup oferece uma solução de backup totalmente gerenciada e baseada em políticas, simplificando o gerenciamento de backup, permitindo que você atenda aos requisitos de conformidade de backup normativos e de negócios. Para obter mais informações, consulte o whitepaper sobre abordagens de backup e recuperação usando a AWS, disponível em https://d0.awsstatic.com/whitepapers/Backup_and_Recovery_Approaches_Using_AWS.pdf
Recuperação de dados	11.3	Proteger	Proteja os dados de recuperação com controles equivalentes aos dados originais. Criptografia de		Customer	A AWS oferece aos clientes a capacidade de configurar e usar adequadamente as ofertas de serviços da AWS para manter a segurança, a proteção e o backup adequados dos dados dos clientes. A AWS permite que os clientes realizem seus próprios backups usando

			referência ou separação de dados, com base nos requisitos.			serviços como o AWS Backup, que é um serviço de backup totalmente gerenciado que simplifica a centralização e a automatização do backup de dados nos serviços da AWS na Cloud e no local usando o AWS Storage Gateway. Usando o AWS Backup, os clientes podem configurar centralmente políticas de backup e monitorar atividades de backup para recursos da AWS, como volumes do Amazon EBS, bancos de dados do Amazon RDS, tabelas do Amazon DynamoDB, sistemas de arquivos do Amazon EFS e volumes do AWS Storage Gateway. O AWS Backup automatiza e consolida tarefas de backup executadas anteriormente serviço por serviço, eliminando a necessidade de criar scripts personalizados e processos manuais. Com apenas alguns cliques no console do AWS Backup, os clientes podem criar políticas de backup que automatizam as agendas de backup e o gerenciamento de retenção. O AWS Backup oferece uma solução de backup totalmente gerenciada e baseada em políticas, simplificando o gerenciamento de backup, permitindo que você atenda aos requisitos de conformidade de backup normativos e de negócios. Para obter mais informações, consulte o whitepaper sobre abordagens de backup e recuperação usando a AWS, disponível em https://d0.awsstatic.com/whitepapers/Backup_and_Recovery_Approaches_Using_AWS.pdf
Recuperação de dados	11.4	Recuperar	Estabeleça e mantenha uma instância isolada dos dados de recuperação. Exemplos de implementações incluem destinos de backup de controle de versão por meio de sistemas ou serviços offline, na Cloud ou fora do local.		Customer	A AWS oferece aos clientes a capacidade de configurar e usar adequadamente as ofertas de serviços da AWS para manter a segurança, a proteção e o backup adequados dos dados dos clientes. A AWS permite que os clientes realizem seus próprios backups usando serviços como o AWS Backup, que é um serviço de backup totalmente gerenciado que simplifica a centralização e a automatização do backup de dados nos serviços da AWS na Cloud e no local usando o AWS Storage Gateway. Usando o AWS Backup, os clientes podem configurar centralmente políticas de backup e monitorar atividades de backup para recursos da AWS, como volumes do Amazon EBS, bancos de dados do Amazon RDS, tabelas do Amazon DynamoDB, sistemas de arquivos do Amazon EFS e volumes do AWS Storage Gateway. O AWS Backup automatiza e consolida tarefas de backup executadas anteriormente serviço por serviço, eliminando a necessidade de criar scripts personalizados e processos manuais. Com apenas alguns cliques no console do AWS Backup, os clientes podem criar políticas de backup que automatizam as agendas de backup e o gerenciamento de retenção. O AWS Backup oferece uma solução de backup totalmente gerenciada e baseada em políticas, simplificando o gerenciamento

						de backup, permitindo que você atenda aos requisitos de conformidade de backup normativos e de negócios. Para obter mais informações, consulte o whitepaper sobre abordagens de backup e recuperação usando a AWS, disponível em https://d0.awsstatic.com/whitepapers/Backup_and_Recovery_Approaches_Using_AWS.pdf
Recuperação de dados	11.5	Recuperar	Teste a recuperação de backup trimestralmente, ou com mais frequência, para obter uma amostra de ativos corporativos dentro do escopo.		Customer	A AWS oferece aos clientes a capacidade de configurar e usar adequadamente as ofertas de serviços da AWS para manter a segurança, a proteção e o backup adequados dos dados dos clientes. A AWS permite que os clientes realizem seus próprios backups usando serviços como o AWS Backup, que é um serviço de backup totalmente gerenciado que simplifica a centralização e a automatização do backup de dados nos serviços da AWS na Cloud e no local usando o AWS Storage Gateway. Usando o AWS Backup, os clientes podem configurar centralmente políticas de backup e monitorar atividades de backup para recursos da AWS, como volumes do Amazon EBS, bancos de dados do Amazon RDS, tabelas do Amazon DynamoDB, sistemas de arquivos do Amazon EFS e volumes do AWS Storage Gateway. O AWS Backup automatiza e consolida tarefas de backup executadas anteriormente serviço por serviço, eliminando a necessidade de criar scripts personalizados e processos manuais. Com apenas alguns cliques no console do AWS Backup, os clientes podem criar políticas de backup que automatizam as agendas de backup e o gerenciamento de retenção. O AWS Backup oferece uma solução de backup totalmente gerenciada e baseada em políticas, simplificando o gerenciamento de backup, permitindo que você atenda aos requisitos de conformidade de backup normativos e de negócios. Para obter mais informações, consulte o whitepaper sobre abordagens de backup e recuperação usando a AWS, disponível em https://d0.awsstatic.com/whitepapers/Backup_and_Recovery_Approaches_Using_AWS.pdf
Gerenciamento de infraestrutura de rede	12.1	Proteger	Garanta que a infraestrutura de rede seja mantida atualizada.	AWS	Cliente	As equipes de segurança da AWS assinam feeds de notícias sobre as falhas aplicáveis do fornecedor e monitoram proativamente os sites dos fornecedores e outros veículos relevantes para novos patches. Os dispositivos de firewall são configurados para restringir o acesso às redes

			Exemplos de implementações incluem a execução da versão estável mais recente do software e/ou o uso de ofertas de rede como serviço (NaaS) atualmente suportadas. Analise as versões de software mensalmente, ou com mais frequência, para verificar o suporte de software.			corporativas e de produção da AWS. As configurações dessas políticas de firewall são mantidas usando um envio automático de um servidor pai a cada 24 horas. Todas as alterações nas políticas de firewall são analisadas e aprovadas. Os clientes da AWS são responsáveis por configurar a segurança de rede em seu ambiente Amazon VPC.
Gerenciamento de infraestrutura de rede	12.2	Proteger	Estabeleça e mantenha uma arquitetura de rede segura. Uma arquitetura de rede segura deve abordar, no mínimo, a segmentação, o menor privilégio e a disponibilidade.	AWS	Cliente	Para permitir um monitoramento mais abrangente das comunicações de entrada e saída e do tráfego de rede, a AWS colocou estrategicamente um número limitado de pontos de acesso à Cloud AWS. Esses pontos de acesso do cliente são chamados de endpoints de API e permitem acesso HTTP seguro (HTTPS), o que permite que os clientes estabeleçam uma sessão de comunicação segura com suas instâncias de armazenamento ou computação na AWS. Para oferecer suporte a clientes com requisitos criptográficos FIPS, os balanceadores de carga de terminação Secure Sockets Layer (SSL) no AWS GovCloud (EUA) estão em conformidade com o FIPS 140-2. Além disso, a AWS implementou dispositivos de rede dedicados ao gerenciamento de comunicações de interface com provedores de serviços de Internet (ISPs). A AWS emprega uma conexão redundante com mais de um serviço de comunicação em cada borda da rede da AWS voltada para a Internet. Cada uma dessas conexões tem dispositivos de rede dedicados. Os clientes da AWS são responsáveis pela configuração de grupos de segurança e ACLs de rede da Amazon VPC.
Gerenciamento de infraestrutura de rede	12.3	Proteger	Gerenciar a infraestrutura de rede com segurança.	AWS	Cliente	Para permitir um monitoramento mais abrangente das comunicações de entrada e saída e do tráfego de rede, a AWS colocou estrategicamente um número limitado de pontos de acesso à Cloud AWS. Esses pontos de acesso do cliente são chamados de endpoints de API e

			Exemplos de implementações incluem infraestrutura controlada por versão como código e o uso de protocolos de rede seguros, como SSH e HTTPS.			permitem acesso HTTP seguro (HTTPS), o que permite que os clientes estabeleçam uma sessão de comunicação segura com suas instâncias de armazenamento ou computação na AWS. Para oferecer suporte a clientes com requisitos criptográficos FIPS, os balanceadores de carga de terminação Secure Sockets Layer (SSL) no AWS GovCloud (EUA) estão em conformidade com o FIPS 140-2. Além disso, a AWS implementou dispositivos de rede dedicados ao gerenciamento de comunicações de interface com provedores de serviços de Internet (ISPs). A AWS emprega uma conexão redundante com mais de um serviço de comunicação em cada borda da rede da AWS voltada para a Internet. Cada uma dessas conexões tem dispositivos de rede dedicados. Os clientes da AWS são responsáveis pela configuração de grupos de segurança e ACLs de rede da Amazon VPC.
Gerenciamento de infraestrutura de rede	12.4	Identificar	Estabelecer e manter diagrama (s) de arquitetura e/ou outra documentação do sistema de rede. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças corporativas significativas que possam afetar essa Proteção.	AWS	Cliente	A AWS estabelece, mantém e atualiza a documentação, incluindo o (s) diagrama (s) de arquitetura para seu sistema de rede interna. A AWS comunica seus requisitos de sistema aos clientes e como começar a usar os serviços da AWS na forma de guias do usuário, guias do desenvolvedor, referências de API, tutoriais específicos de serviços ou kits de ferramentas do SDK. Mais informações sobre a documentação da AWS podem ser encontradas em https://docs.aws.amazon.com/. Esses recursos ajudam os clientes a arquitetar os serviços da AWS para satisfazer suas necessidades de negócios. Os clientes da AWS são responsáveis por estabelecer termos e condições com outras organizações que possuem, operam e/ou mantêm sistemas de informação externos. Consistente com quaisquer relações de confiança estabelecidas com essas organizações externas e de acordo com sua política de controle de acesso, os clientes da AWS são responsáveis por autorizar os indivíduos a: 1) Acessar seu sistema a partir de um sistema de informações externo e 2) Processar, armazenar ou transmitir a organização informações controladas usando sistemas de informação externos.
Gerenciamento de infraestrutura de rede	12.5	Proteger	Centralize a rede AAA.	AWS	Cliente	A AWS estabelece, mantém e atualiza a documentação, incluindo o (s) diagrama (s) de arquitetura para seu sistema de rede interna. A AWS comunica seus requisitos de sistema aos clientes e como começar a usar os serviços da AWS na forma de guias do usuário, guias do desenvolvedor, referências de API, tutoriais específicos de serviços ou kits de ferramentas do SDK. Mais informações sobre a documentação da AWS podem ser encontradas em https://docs.aws.amazon.com/. Esses recursos ajudam os clientes a arquitetar os serviços da AWS para satisfazer suas necessidades de negócios.

						Os clientes da AWS são responsáveis por estabelecer termos e condições com outras organizações que possuem, operam e/ou mantêm sistemas de informação externos. Consistente com quaisquer relações de confiança estabelecidas com essas organizações externas e de acordo com sua política de controle de acesso, os clientes da AWS são responsáveis por autorizar os indivíduos a: 1) Acessar seu sistema a partir de um sistema de informações externo e 2) Processar, armazenar ou transmitir a organização informações controladas usando sistemas de informação externos.
Gerenciamento de infraestrutura de rede	12.6	Proteger	Use protocolos de comunicação e gerenciamento de rede seguros (por exemplo, 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise ou superior).	AWS	Cliente	Não há redes sem fio dentro dos limites do sistema da AWS. A AWS monitora continuamente redes sem fio para detectar dispositivos não autorizados ou não autorizados. Os clientes da AWS são responsáveis por configurar seus sistemas para impor um bloqueio de sessão após um período de inatividade definido em sua política de controle de acesso ou ao receber uma solicitação de um usuário. Esse bloqueio de sessão deve ser mantido até que o usuário restabeleça o acesso usando os procedimentos estabelecidos de identificação e autenticação. Os clientes da AWS são responsáveis por identificar as ações do usuário que podem ser executadas em seus sistemas sem identificação ou autenticação e documentar a justificativa de suporte para essas ações em seu plano de segurança. Os clientes da AWS são responsáveis por implementar mecanismos para proteger a confidencialidade e a integridade das informações transmitidas.
Gerenciamento de infraestrutura de rede	12.7	Proteger	Exija que os usuários se autentiquem em serviços de autenticação e VPN gerenciados pela empresa antes de acessar os recursos corporativos nos		Cliente	Os clientes da AWS são responsáveis por estabelecer e documentar restrições de uso, requisitos de configuração/conexão e orientações de implementação para cada tipo de acesso remoto permitido a seus sistemas de acordo com sua política de controle de acesso. Os clientes da AWS são responsáveis por autorizar o acesso remoto aos seus sistemas antes de permitir essas conexões.

			dispositivos do usuário final.			
Gerenciamento de infraestrutura de rede	12.8	Proteger	Estabeleça e mantenha recursos de computação dedicados, separados física ou logicamente, para todas as tarefas administrativas ou que exijam acesso administrativo. Os recursos de computação devem ser segmentados a partir da rede primária da empresa e não ter acesso à Internet.		Cliente	Os clientes da AWS são responsáveis por limitar o número de sessões simultâneas aos seus sistemas de acordo com sua política de controle de acesso. Os clientes da AWS são responsáveis por configurar seus sistemas e todos os sistemas interconectados para aplicar suas políticas de fluxo de informações aprovadas. Isso pode ser feito por meio da configuração de listas de controle de acesso (ACL) de rede do Amazon Virtual Private Cloud (Amazon VPC) para controlar o tráfego de entrada/saída no nível da sub-rede e grupos de segurança da Amazon VPC para controlar o tráfego no nível da instância.
Monitoramento e defesa de rede	13.1	Detectar	Centralize os alertas de eventos de segurança em todos os ativos corporativos para correlação e análise de logs. A implementação de práticas recomendadas requer o uso de um SIEM, que inclui alertas de correlação de eventos definidos pelo fornecedor. Uma plataforma de análise de log		Cliente	Os clientes da AWS são responsáveis por gerenciar contas associadas aos seus aplicativos hospedados na AWS. Os clientes da AWS são responsáveis por usar corretamente o AWS Identity and Access Management (IAM) para criar e gerenciar contas de usuário e impor o acesso em suas instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e em todos os aplicativos que instalam. Os clientes da AWS no contexto do gerenciamento de suas contas de usuário são responsáveis por: 1) Identificar e selecionar contas do sistema; 2) Atribuir gerentes de conta para contas do sistema; 3) Especificar usuários autorizados, associação a grupos e funções, autorizações de acesso e outros atributos, conforme necessário para cada conta; 4) Exigir aprovações de pessoal ou funções definidas pelo cliente para solicitações de criação de

			configurada com alertas de correlação relevantes para a segurança também satisfaz esse Safeguard.			conta; 5) Monitoramento do uso da conta; 6) Notificar gerentes de conta quando: a) Contas não forem mais necessárias, b) Usuários forem encerrados ou transferidos e c) Uso individual do sistema ou alterações necessárias; 7) Autorização de acesso com base em: a) Uma autorização de acesso válida, b) Uso pretendido do sistema e c) Outros atributos, conforme exigido por sua organização ou missão associada/funções de negócios; 8) Revisar as contas quanto à conformidade com os requisitos de gerenciamento de contas em uma frequência definida por sua organização; e 9) Estabelecer um processo para reemitir credenciais de conta compartilhada/de grupo quando indivíduos são removidos do grupo.
Monitoramento e defesa de rede	13.2	Detectar	Implante uma solução de detecção de intrusão baseada em host em ativos corporativos, quando apropriado e/ou suportado.		Cliente	Os clientes da AWS são responsáveis por gerenciar contas associadas aos seus aplicativos hospedados na AWS. Os clientes da AWS são responsáveis por usar corretamente o AWS Identity and Access Management (IAM) para criar e gerenciar contas de usuário e impor o acesso em suas instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e em todos os aplicativos que instalam. Os clientes da AWS no contexto do gerenciamento de suas contas de usuário são responsáveis por: 1) Identificar e selecionar contas do sistema; 2) Atribuir gerentes de conta para contas do sistema; 3) Especificar usuários autorizados, associação a grupos e funções, autorizações de acesso e outros atributos, conforme necessário para cada conta; 4) Exigir aprovações de pessoal ou funções definidas pelo cliente para solicitações de criação de conta; 5) Monitoramento do uso da conta; 6) Notificar gerentes de conta quando: a) Contas não forem mais necessárias, b) Usuários forem encerrados ou transferidos e c) Uso individual do sistema ou alterações necessárias; 7) Autorização de acesso com base em: a) Uma autorização de acesso válida, b) Uso pretendido do sistema e c) Outros atributos, conforme exigido por sua organização ou missão associada/funções de negócios; 8) Revisar as contas quanto à conformidade com os requisitos de gerenciamento de contas em uma frequência definida por sua organização; e 9) Estabelecer um processo para reemitir credenciais de conta compartilhada/de grupo quando indivíduos são removidos do grupo.
Monitoramento e defesa de	13.3	Detectar	Implante uma solução de		Cliente	

rede			detecção de intrusão de rede em ativos corporativos, quando apropriado. Exemplos de implementações incluem o uso de um Sistema de Detecção de Intrusão de Rede (NIDS) ou um serviço equivalente de provedor de serviços em Cloud (CSP).			Os clientes da AWS são responsáveis por gerenciar contas associadas aos seus aplicativos hospedados na AWS. Os clientes da AWS são responsáveis por usar corretamente o AWS Identity and Access Management (IAM) para criar e gerenciar contas de usuário e impor o acesso em suas instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e em todos os aplicativos que instalam. Os clientes da AWS no contexto do gerenciamento de suas contas de usuário são responsáveis por: 1) Identificar e selecionar contas do sistema; 2) Atribuir gerentes de conta para contas do sistema; 3) Especificar usuários autorizados, associação a grupos e funções, autorizações de acesso e outros atributos, conforme necessário para cada conta; 4) Exigir aprovações de pessoal ou funções definidas pelo cliente para solicitações de criação de conta; 5) Monitoramento do uso da conta; 6) Notificar gerentes de conta quando: a) Contas não forem mais necessárias, b) Usuários forem encerrados ou transferidos e c) Uso individual do sistema ou alterações necessárias; 7) Autorização de acesso com base em: a) Uma autorização de acesso válida, b) Uso pretendido do sistema e c) Outros atributos, conforme exigido por sua organização ou missão associada/funções de negócios; 8) Revisar as contas quanto à conformidade com os requisitos de gerenciamento de contas em uma frequência definida por sua organização; e 9) Estabelecer um processo para reemitir credenciais de conta compartilhada/de grupo quando indivíduos são removidos do grupo.
Monitoramento e defesa de rede	13.4	Proteger	Execute a filtragem de tráfego entre segmentos de rede, quando apropriado.	AWS	Cliente	Existem várias malhas de rede na AWS, cada uma separada por dispositivos de proteção de limites que controlam o fluxo de informações entre malhas. O fluxo de informações entre os tecidos é estabelecido por autorizações aprovadas, que existem como ACLs residentes nesses dispositivos. As ACLs são definidas e aprovadas pela equipe apropriada de segurança da informação da Amazon e gerenciadas e implantadas usando a ferramenta de gerenciamento de ACL da AWS. Conjuntos de regras de firewall aprovados e listas de controle de acesso entre malhas de rede restringem o fluxo de informações para serviços específicos do sistema de informações. ACLs e conjuntos de regras são revisados e aprovados e enviados automaticamente para dispositivos de proteção de limites periodicamente (pelo menos a cada 24 horas) para garantir que os conjuntos de regras e as listas de controle de acesso estejam atualizados.

						A AWS implementa o menor privilégio em todos os seus componentes de infraestrutura. A AWS proíbe todas as portas e protocolos que não tenham um objetivo comercial específico. A AWS segue uma abordagem rigorosa para a implementação mínima apenas dos recursos e funções essenciais para o uso do dispositivo. A varredura de rede é executada e todas as portas ou protocolos desnecessários em uso são corrigidos. Os clientes da AWS são responsáveis por configurar seu sistema para fornecer apenas recursos essenciais e proibir ou restringir o uso de funções, portas, protocolos e/ou serviços, conforme definido em sua política de gerenciamento de configuração. Os clientes da AWS são responsáveis por implementar mecanismos de proteção de limites nos principais limites internos e externos do sistema para controlar o fluxo de informações em seus sistemas. Os clientes da AWS são responsáveis por revisar seus sistemas em uma frequência definida por sua política de gerenciamento de configuração para identificar e desativar funções, portas, protocolos e serviços desnecessários e/ou não seguros. Os clientes da AWS são responsáveis por configurar seu sistema e todos os sistemas interconectados para aplicar suas políticas de fluxo de informações aprovadas. Isso pode ser feito por meio da configuração de ACLs de rede da Amazon Virtual Private Cloud (Amazon VPC) para controlar o tráfego de entrada/saída no nível da sub-rede e grupos de segurança da Amazon VPC para controlar o tráfego no nível da instância. Para obter mais informações, consulte https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html
Monitoramento e defesa de rede	13.5	Proteger	Gerencie o controle de acesso para ativos conectando-se remotamente aos recursos da empresa. Determine a quantidade de acesso aos recursos corporativos com base em: software antimalware atualizado instalado,	AWS	Cliente	O acesso remoto aos ambientes de produção da AWS é limitado a grupos de segurança definidos. A adição de membros em um grupo deve ser revisada e aprovada por indivíduos autorizados que confirmam a necessidade de acesso do usuário ao ambiente. O acesso remoto requer autenticação multifator em um canal criptográfico aprovado para autenticação. A AWS emprega mecanismos automatizados para facilitar o monitoramento e o controle de métodos de acesso remoto. A auditoria ocorre nos sistemas e dispositivos, que são agregados e armazenados em uma ferramenta proprietária para análise e investigação de incidentes. O ambiente operacional da AWS, para incluir configuração de rede e segurança, é considerado informação confidencial e deve ser protegido pelos funcionários de acordo

			conformidade de configuração com o processo de configuração segura da empresa e garantia de que o sistema operacional e os aplicativos estejam atualizados.			com as políticas de classificação de dados da AWS. Todas as tentativas de acesso administrativo remoto são registradas e limitadas a um número específico de tentativas. Os registros de auditoria são analisados pela equipe de segurança da AWS em busca de tentativas não autorizadas ou atividades suspeitas. Se alguma atividade suspeita é detectada, os procedimentos de resposta a incidentes são iniciados. Os clientes da AWS são responsáveis por estabelecer e documentar restrições de uso, requisitos de configuração/conexão e orientações de implementação para cada tipo de acesso remoto permitido a seus sistemas (incluindo autenticação multifator, se exigido pela organização) de acordo com seu acesso política de controle. Os clientes da AWS são responsáveis por autorizar o acesso remoto aos seus sistemas antes de permitir essas conexões. Os clientes da AWS são responsáveis por implementar o monitoramento e o controle do acesso remoto e pela implementação de mecanismos criptográficos para proteger a confidencialidade e a integridade das sessões de acesso remoto.
Monitoramento e defesa de rede	13.6	Detectar	Colete registros de fluxo de tráfego de rede e/ou tráfego de rede para revisar e alertar sobre os dispositivos de rede.		Cliente	Os clientes mantêm o controle do conteúdo armazenado ou processado usando a AWS, incluindo controle sobre como esse conteúdo é protegido e quem pode acessar e corrigir esse conteúdo. Os clientes podem manter uma variedade de registros e automatizar as notificações. A AWS oferece serviços como o Amazon CloudWatch para monitorar os recursos da Cloud da AWS e os aplicativos que você executa na AWS. Os clientes podem usar o Amazon CloudWatch para coletar e rastrear métricas, coletar e monitorar arquivos de log, definir alarmes, enviar notificações e reagir automaticamente a alterações em seus recursos da AWS. Com o AWS CloudTrail, você pode registrar, monitorar continuamente e reter eventos relacionados a chamadas de interface de programação de aplicativos (API) em toda a infraestrutura da AWS. Para obter mais informações sobre registro e monitoramento, visite https://docs.aws.amazon.com/whitepapers/latest/aws-security-best-practices/
Monitoramento e defesa de rede	13.7	Proteger	Implante uma solução de prevenção de		Customer	Os clientes da AWS são responsáveis pela implementação e configuração de mecanismos de monitoramento e proteção baseados em host, incluindo software antivírus e antimalware, ferramentas de verificação de integridade,

			intrusões baseada em host em ativos corporativos, quando apropriado e/ou suportado. Exemplos de implementações incluem o uso de um cliente Endpoint Detection and Response (EDR) ou um agente IPS baseado em host.			detecção/prevenção de intrusão baseada em host e proteção contra spam. Os clientes da AWS são responsáveis por todas as verificações, testes de penetração, monitoramento de integridade de arquivos e detecção de intrusão para suas instâncias e aplicativos do Amazon EC2 e do Amazon ECS. As varreduras devem incluir endereços IP de clientes e não endpoints da AWS. Os endpoints da AWS são testados como parte das verificações de vulnerabilidade de conformidade da AWS. As equipes de segurança da AWS também se inscrevem em feeds de notícias sobre falhas de fornecedores aplicáveis e monitoram proativamente os sites dos fornecedores e outros veículos relevantes em busca de novos patches. Os clientes da AWS também podem relatar problemas para a AWS por meio do site de relatórios de vulnerabilidades da AWS em http://aws.amazon.com/security/vulnerability-reporting/.
Monitoramento e defesa de rede	13.8	Proteger	Implante uma solução de prevenção contra intrusões de rede, quando apropriado. Exemplos de implementações incluem o uso de um Sistema de Prevenção de Intrusões de Rede (NIPS) ou serviço CSP equivalente.		Customer	Os clientes da AWS são responsáveis pela implementação e configuração de mecanismos de monitoramento e proteção baseados em host, incluindo software antivírus e antimalware, ferramentas de verificação de integridade, detecção/prevenção de intrusão baseada em host e proteção contra spam. Os clientes da AWS são responsáveis por todas as verificações, testes de penetração, monitoramento de integridade de arquivos e detecção de intrusão para suas instâncias e aplicativos do Amazon EC2 e do Amazon ECS. As varreduras devem incluir endereços IP de clientes e não endpoints da AWS. Os endpoints da AWS são testados como parte das verificações de vulnerabilidade de conformidade da AWS. As equipes de segurança da AWS também se inscrevem em feeds de notícias sobre falhas de fornecedores aplicáveis e monitoram proativamente os sites dos fornecedores e outros veículos relevantes em busca de novos patches. Os clientes da AWS também podem relatar problemas para a AWS por meio do site de relatórios de vulnerabilidades da AWS em http://aws.amazon.com/security/vulnerability-reporting/.
Monitoramento e defesa de rede	13.9	Proteger	Implante o controle de acesso no nível da porta. O controle de acesso no nível da porta	AWS	Cliente	Existem várias malhas de rede na Amazon, cada uma separada por dispositivos de proteção de limites que controlam o fluxo de informações entre malhas. O fluxo de informações entre os tecidos é estabelecido por autorizações aprovadas, que existem como ACLs residentes nesses dispositivos. As ACLs são definidas e aprovadas pela equipe apropriada de

			utiliza protocolos de controle de acesso de rede 802.1x ou similares, como certificados, e pode incorporar autenticação de usuário e/ou dispositivo.			segurança da informação da Amazon e gerenciadas e implantadas usando a ferramenta de gerenciamento de ACL da AWS. Conjuntos de regras de firewall aprovados e listas de controle de acesso entre malhas de rede restringem o fluxo de informações para serviços específicos do sistema de informações. ACLs e conjuntos de regras são revisados e aprovados e enviados automaticamente para dispositivos de proteção de limites periodicamente (pelo menos a cada 24 horas) para garantir que os conjuntos de regras e as listas de controle de acesso estejam atualizados. A AWS implementa o menor privilégio em todos os seus componentes de infraestrutura. A AWS proíbe todas as portas e protocolos que não tenham um objetivo comercial específico. A AWS segue uma abordagem rigorosa para a implementação mínima apenas dos recursos e funções essenciais para o uso do dispositivo. A varredura de rede é executada e todas as portas ou protocolos desnecessários em uso são corrigidos. Os clientes da AWS são responsáveis por configurar seu sistema para fornecer apenas recursos essenciais e proibir ou restringir o uso de funções, portas, protocolos e/ou serviços, conforme definido em sua política de gerenciamento de configuração. Os clientes da AWS são responsáveis por implementar mecanismos de proteção de limites nos principais limites internos e externos do sistema para controlar o fluxo de informações em seus sistemas. Os clientes da AWS são responsáveis por revisar seus sistemas em uma frequência definida por sua política de gerenciamento de configuração para identificar e desativar funções, portas, protocolos e serviços desnecessários e/ou não seguros. Os clientes da AWS são responsáveis por configurar seu sistema e todos os sistemas interconectados para aplicar suas políticas de fluxo de informações aprovadas. Isso pode ser feito por meio da configuração de ACLs de rede da Amazon Virtual Private Cloud (Amazon VPC) para controlar o tráfego de entrada/saída no nível da sub-rede e grupos de segurança da Amazon VPC para controlar o tráfego no nível da instância. Para obter mais informações, consulte https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html
Monitoramento e defesa de rede	13.10	Proteger	Execute a filtragem da camada de aplicação. Exemplos de	AWS	Cliente	A rede da AWS consiste em instalações internas de datacenter, servidores, equipamentos de rede e sistemas de software host que estão sob o controle da AWS e são usados para fornecer os serviços.

			implementações incluem um proxy de filtragem, um firewall da camada de aplicativo ou um gateway.			A rede da AWS oferece proteção significativa contra problemas de segurança de rede tradicionais. Por exemplo: - Ataques distribuídos de negação de serviço (DDoS). Os endpoints da AWS API são hospedados em uma grande infraestrutura à escala da Internet e usam técnicas proprietárias de mitigação de DDoS. Além disso, as redes da AWS têm hospedagem múltipla em vários provedores para alcançar a diversidade de acesso à Internet. - Falsificação de IP. A infraestrutura de firewall baseada em host controlada pela AWS não permitirá que uma instância envie tráfego com um endereço IP ou MAC de origem diferente do seu. - Sniffing de pacotes por outros inquilinos. As instâncias virtuais são projetadas para impedir que outras instâncias executadas em modo promíscuo recebam ou “farejam” o tráfego destinado a uma instância virtual diferente. Embora os clientes possam colocar interfaces no modo promíscuo, o hipervisor não entregará nenhum tráfego que não seja endereçado a eles. Mesmo duas instâncias virtuais pertencentes ao mesmo cliente localizadas no mesmo host físico não podem ouvir o tráfego uma da outra. Embora o Amazon EC2 ofereça proteção contra um cliente que tenta visualizar os dados de outro, como prática padrão, os clientes podem criptografar tráfego confidencial. Além disso, os dispositivos de firewall são configurados para restringir o acesso às redes corporativas e de produção da AWS. As configurações dessas políticas de firewall são mantidas usando um envio automático de um servidor pai a cada 24 horas. Todas as alterações nas políticas de firewall são analisadas e aprovadas pela equipa da AWS. Os clientes da AWS são responsáveis por configurar a segurança de rede em seu ambiente Amazon VPC.
Monitoramento e defesa de rede	13.11	Detectar	Ajuste os limites de alertas de eventos de segurança mensalmente ou	AWS	Cliente	A AWS notificará os clientes sobre uma violação de segurança de acordo com os termos descritos no contrato de serviço com a AWS. O compromisso da AWS com todos os clientes da AWS é o seguinte:

			com mais frequência.			Se a AWS tomar conhecimento de qualquer acesso ilegal ou não autorizado a quaisquer dados do cliente (ou seja, quaisquer dados pessoais carregados na conta da AWS de um cliente) no equipamento da AWS ou nas instalações da AWS e esse acesso ilegal ou não autorizado resultar em perda, divulgação ou alteração dos dados do cliente, a AWS prontamente notificar o cliente e tomar medidas razoáveis para reduzir os efeitos desse incidente de segurança. A AWS define, administra e monitora a segurança da infraestrutura de Cloud subjacente (ou seja, o hardware, as instalações que abrigam o hardware e a infraestrutura de rede). Como a AWS gerencia a infraestrutura e os controles de segurança que se aplicam a ela, a AWS pode: • Identificar possíveis incidentes que afetam a infraestrutura. • Determine se algum acesso aos dados do cliente resultou de um incidente. • Determinar se o acesso foi realmente ilegal ou não autorizado (seria não autorizado se violasse as políticas de segurança da AWS). Se um incidente ocorrer dentro da esfera de conhecimento e controle da AWS e esse incidente resultar em perda, divulgação ou alteração do conteúdo do cliente, a AWS notificará o cliente imediatamente. A AWS faz isso independentemente de o conteúdo do cliente ser confidencial ou não, porque a AWS não sabe qual é o conteúdo do cliente e protege todo o conteúdo do cliente da mesma maneira robusta. Para facilitar uma resposta e uma notificação oportunas, os clientes da AWS devem garantir que suas contas da AWS sejam atualizadas com os detalhes de contato adequados e, especialmente, que os contatos de segurança são precisos e direcionados para uma conta de e-mail que é monitorada regularmente. Os clientes da AWS devem implementar as seguintes melhores práticas para proteção contra violações de segurança: • Use criptografia para proteger dados em repouso e em trânsito.

						• Configure seus sistemas com segurança adequada. • Gerencie contas da AWS e usuários, grupos e funções do IAM para implementar permissões de privilégio mínimo. • Use ferramentas de monitoramento como o Amazon CloudWatch para rastrear quando suas informações são acessadas e por quem. Os clientes da AWS também devem visitar a página Best Practices for Security, Identity and Compliance em https://aws.amazon.com/architecture/security-identity-compliance/?cards-all.sort-by=item.additionalFields.sortDate&cards-all.sort-order=desc, que inclui detalhes de cada um dos itens acima pontos listados
Treinamento de habilidades e conscientização de segurança	14.1	Proteger	Estabelecer e manter um programa de conscientização de segurança. O objetivo de um programa de conscientização sobre segurança é educar a força de trabalho da empresa sobre como interagir com ativos e dados corporativos de maneira segura. Realizar treinamentos contratados e, no mínimo, anualmente. Revise e atualize o conteúdo anualmente ou quando ocorrerem mudanças corporativas significativas que	AWS	Cliente	Os clientes da AWS são responsáveis por fornecer treinamento básico de conscientização de segurança aos usuários (incluindo gerentes, executivos seniores e contratados): 1) Como parte do treinamento inicial para novos usuários, 2) Quando exigido por mudanças no sistema de informações e 3) Em uma frequência definida pela organização posteriormente. A AWS estabeleceu e comunicou políticas e estruturas de segurança da informação que integraram a estrutura certificável ISO 27001 com base nos controles da ISO 27002, nos Princípios de Serviços de Confiança do American Institute of Certified Public Accountants (AICPA), no PCI DSS v3.1 e no National Institute of Standards e Publicação 800-53 da Technology (NIST) (Controles de segurança recomendados para sistemas de informação federais). A AWS gerencia relacionamentos com terceiros em alinhamento com os padrões ISO 27001. Os requisitos de terceiros da AWS são analisados por auditores externos independentes durante auditorias para nossa conformidade com PCI DSS, ISO 27001 e FedRAMP.

			possam afetar essa Proteção.			
Treinamento de habilidades e conscientização de segurança	14.2	Proteger	Treine os membros da força de trabalho para reconhecer ataques de engenharia social, como phishing, pré-mensagens de texto e utilização não autorizada.	AWS	Cliente	Os clientes da AWS são responsáveis por fornecer treinamento básico de conscientização de segurança aos usuários (incluindo gerentes, executivos seniores e contratados): 1) Como parte do treinamento inicial para novos usuários, 2) Quando exigido por mudanças no sistema de informações e 3) Em uma frequência definida pela organização posteriormente. A AWS estabeleceu e comunicou políticas e estruturas de segurança da informação que integraram a estrutura certificável ISO 27001 com base nos controles da ISO 27002, nos Princípios de Serviços de Confiança do American Institute of Certified Public Accountants (AICPA), no PCI DSS v3.1 e no National Institute of Standards e Publicação 800-53 da Technology (NIST) (Controles de segurança recomendados para sistemas de informação federais). A AWS gerencia relacionamentos com terceiros em alinhamento com os padrões ISO 27001. Os requisitos de terceiros da AWS são analisados por auditores externos independentes durante auditorias para nossa conformidade com PCI DSS, ISO 27001 e FedRAMP.
Treinamento de habilidades e conscientização de segurança	14.3	Proteger	Treine os membros da força de trabalho nas melhores práticas de autenticação Os tópicos de exemplo incluem MFA, composição de senhas e gerenciamento de credenciais.	AWS	Cliente	Os clientes da AWS são responsáveis por fornecer treinamento básico de conscientização de segurança aos usuários (incluindo gerentes, executivos seniores e contratados): 1) Como parte do treinamento inicial para novos usuários, 2) Quando exigido por mudanças no sistema de informações e 3) Em uma frequência definida pela organização posteriormente. A AWS estabeleceu e comunicou políticas e estruturas de segurança da informação que integraram a estrutura certificável ISO 27001 com base nos controles da ISO 27002, nos Princípios de Serviços de Confiança do American Institute of Certified Public Accountants (AICPA), no PCI DSS v3.1 e no National Institute of Standards e Publicação 800-53 da Technology (NIST) (Controles de segurança recomendados para sistemas de informação federais). A AWS gerencia relacionamentos com terceiros em alinhamento com os padrões ISO 27001. Os requisitos de terceiros da AWS são analisados por auditores externos independentes durante auditorias para nossa conformidade com PCI DSS, ISO 27001 e FedRAMP.
Treinamento de habilidades e conscientização de	14.4	Proteger	Treine os membros da força de trabalho sobre como identificar e armazenar,	AWS	Cliente	Os clientes da AWS são responsáveis por fornecer treinamento básico de conscientização de segurança aos usuários (incluindo gerentes, executivos seniores e contratados): 1) Como parte do treinamento inicial para novos usuários, 2) Quando exigido por mudanças no sistema de informações e 3) Em uma frequência definida pela organização posteriormente.

segurança			transferir, arquivar e destruir dados confidenciais adequadamente. Isso também inclui o treinamento dos membros da força de trabalho sobre as melhores práticas de tela clara e de mesa, como bloquear a tela quando eles se afastam de seus ativos corporativos, apagar quadros brancos físicos e virtuais no final das reuniões e armazenar dados e ativos com segurança.			A AWS estabeleceu e comunicou políticas e estruturas de segurança da informação que integraram a estrutura certificável ISO 27001 com base nos controles da ISO 27002, nos Princípios de Serviços de Confiança do American Institute of Certified Public Accountants (AICPA), no PCI DSS v3.1 e no National Institute of Standards e Publicação 800-53 da Technology (NIST) (Controles de segurança recomendados para sistemas de informação federais). A AWS gerencia relacionamentos com terceiros em alinhamento com os padrões ISO 27001. Os requisitos de terceiros da AWS são analisados por auditores externos independentes durante auditorias para nossa conformidade com PCI DSS, ISO 27001 e FedRAMP.
Treinamento de habilidades e conscientização de segurança	14.5	Proteger	Treine os membros da força de trabalho para estarem cientes das causas da exposição não intencional de dados. Os tópicos de exemplo incluem entrega incorreta de dados confidenciais, perda de um dispositivo portátil de usuário final ou publicação de dados para públicos indesejados.	AWS	Cliente	Os clientes da AWS são responsáveis por fornecer treinamento básico de conscientização de segurança aos usuários (incluindo gerentes, executivos seniores e contratados): 1) Como parte do treinamento inicial para novos usuários, 2) Quando exigido por mudanças no sistema de informações e 3) Em uma frequência definida pela organização posteriormente. A AWS estabeleceu e comunicou políticas e estruturas de segurança da informação que integraram a estrutura certificável ISO 27001 com base nos controles da ISO 27002, nos Princípios de Serviços de Confiança do American Institute of Certified Public Accountants (AICPA), no PCI DSS v3.1 e no National Institute of Standards e Publicação 800-53 da Technology (NIST) (Controles de segurança recomendados para sistemas de informação federais). A AWS gerencia relacionamentos com terceiros em alinhamento com os padrões ISO 27001. Os requisitos de terceiros da AWS são analisados por auditores externos independentes durante auditorias para nossa conformidade com PCI DSS, ISO 27001 e FedRAMP.

Treinamento de habilidades e conscientização de segurança	14.6	Proteger	Treine os membros da força de trabalho para serem capazes de reconhecer um possível incidente e relatar esse incidente.	AWS	Cliente	Os clientes da AWS são responsáveis por fornecer treinamento básico de conscientização de segurança aos usuários (incluindo gerentes, executivos seniores e contratados): 1) Como parte do treinamento inicial para novos usuários, 2) Quando exigido por mudanças no sistema de informações e 3) Em uma frequência definida pela organização posteriormente. A AWS estabeleceu e comunicou políticas e estruturas de segurança da informação que integraram a estrutura certificável ISO 27001 com base nos controles da ISO 27002, nos Princípios de Serviços de Confiança do American Institute of Certified Public Accountants (AICPA), no PCI DSS v3.1 e no National Institute of Standards e Publicação 800-53 da Technology (NIST) (Controles de segurança recomendados para sistemas de informação federais). A AWS gerencia relacionamentos com terceiros em alinhamento com os padrões ISO 27001. Os requisitos de terceiros da AWS são analisados por auditores externos independentes durante auditorias para nossa conformidade com PCI DSS, ISO 27001 e FedRAMP.
Treinamento de habilidades e conscientização de segurança	14.7	Proteger	Treine a força de trabalho para entender como verificar e relatar patches de software desatualizados ou quaisquer falhas em processos e ferramentas automatizados. Parte desse treinamento deve incluir a notificação da equipe de TI sobre quaisquer falhas em processos e ferramentas automatizados.	AWS	Cliente	Os clientes da AWS são responsáveis por fornecer treinamento básico de conscientização de segurança aos usuários (incluindo gerentes, executivos seniores e contratados): 1) Como parte do treinamento inicial para novos usuários, 2) Quando exigido por mudanças no sistema de informações e 3) Em uma frequência definida pela organização posteriormente. A AWS estabeleceu e comunicou políticas e estruturas de segurança da informação que integraram a estrutura certificável ISO 27001 com base nos controles da ISO 27002, nos Princípios de Serviços de Confiança do American Institute of Certified Public Accountants (AICPA), no PCI DSS v3.1 e no National Institute of Standards e Publicação 800-53 da Technology (NIST) (Controles de segurança recomendados para sistemas de informação federais). A AWS gerencia relacionamentos com terceiros em alinhamento com os padrões ISO 27001. Os requisitos de terceiros da AWS são analisados por auditores externos independentes durante auditorias para nossa conformidade com PCI DSS, ISO 27001 e FedRAMP.
Treinamento de habilidades e	14.8	Proteger	Treine os membros da força de trabalho sobre	AWS	Cliente	Os clientes da AWS são responsáveis por fornecer treinamento básico de conscientização de segurança aos usuários (incluindo gerentes, executivos seniores e contratados): 1) Como parte do treinamento inicial para novos usuários, 2) Quando exigido por mudanças no sistema de informações e 3)

conscientização de segurança			os perigos de se conectar e transmitir dados através de redes inseguras para atividades corporativas. Se a empresa tiver trabalhadores remotos, o treinamento deve incluir orientações para garantir que todos os usuários configurem com segurança sua infraestrutura de rede doméstica.			Em uma frequência definida pela organização posteriormente. A AWS estabeleceu e comunicou políticas e estruturas de segurança da informação que integraram a estrutura certificável ISO 27001 com base nos controles da ISO 27002, nos Princípios de Serviços de Confiança do American Institute of Certified Public Accountants (AICPA), no PCI DSS v3.1 e no National Institute of Standards e Publicação 800-53 da Technology (NIST) (Controles de segurança recomendados para sistemas de informação federais). A AWS gerencia relacionamentos com terceiros em alinhamento com os padrões ISO 27001. Os requisitos de terceiros da AWS são analisados por auditores externos independentes durante auditorias para nossa conformidade com PCI DSS, ISO 27001 e FedRAMP.
Treinamento de habilidades e conscientização de segurança	14.9	Proteger	Conduza treinamento de habilidades e conscientização de segurança específicos da função. Exemplos de implementações incluem cursos de administração de sistemas seguros para profissionais de TI, (OWASP® Top 10) treinamento de conscientização e prevenção de vulnerabilidades para desenvolvedores de aplicativos da web e treinamento avançado de	AWS	Cliente	Os clientes da AWS são responsáveis por fornecer treinamento básico de conscientização de segurança aos usuários (incluindo gerentes, executivos seniores e contratados): 1) Como parte do treinamento inicial para novos usuários, 2) Quando exigido por mudanças no sistema de informações e 3) Em uma frequência definida pela organização posteriormente. A AWS estabeleceu e comunicou políticas e estruturas de segurança da informação que integraram a estrutura certificável ISO 27001 com base nos controles da ISO 27002, nos Princípios de Serviços de Confiança do American Institute of Certified Public Accountants (AICPA), no PCI DSS v3.1 e no National Institute of Standards e Publicação 800-53 da Technology (NIST) (Controles de segurança recomendados para sistemas de informação federais). A AWS gerencia relacionamentos com terceiros em alinhamento com os padrões ISO 27001. Os requisitos de terceiros da AWS são analisados por auditores externos independentes durante auditorias para nossa conformidade com PCI DSS, ISO 27001 e FedRAMP.

			conscientização de engenharia social para funções de alto nível.			
Gerenciamento de provedores de serviços	15.1	Identificar	Estabelecer e manter um inventário dos provedores de serviços. O inventário consiste em listar todos os provedores de serviços conhecidos, incluir classificação (ões) e designar um contato corporativo para cada provedor de serviços. Revise e atualize o inventário anualmente ou quando ocorrerem mudanças significativas na empresa que possam afetar essa Salvaguarda.	AWS	Cliente	A AWS comunica compromissos de serviço a entidades de usuários (clientes da AWS) na forma de acordos de nível de serviço (SLAs), contratos de clientes (https://aws.amazon.com/agreement/), contratos ou por meio da descrição das ofertas de serviço fornecidas on-line por meio do site da AWS. Mais informações sobre os contratos de nível de serviço podem ser encontradas em https://aws.amazon.com/legal/service-level-agreements/. Os clientes da AWS são responsáveis por: 1) Estabelecer requisitos de segurança de pessoal, incluindo funções e responsabilidades de segurança para provedores terceirizados, 2) Exigir que provedores terceirizados cumpram as políticas e procedimentos de segurança de pessoal estabelecidos por sua organização, 3) Documentar o pessoal requisitos de segurança, 4) Exigir que os provedores terceirizados notifiquem o pessoal ou as funções definidas pela organização de quaisquer transferências ou rescisões de pessoal de terceiros que possuam credenciais e/ou crachás organizacionais ou que tenham privilégios do sistema de informações dentro de um período de tempo definido pela organização, e 5) Monitoramento da conformidade do provedor.
Gerenciamento de provedores de serviços	15.2	Identificar	Estabelecer e manter uma política de gerenciamento de provedores de serviços. Certifique-se de que a política aborda a classificação, o inventário, a	AWS	Cliente	A AWS comunica compromissos de serviço a entidades de usuários (clientes da AWS) na forma de acordos de nível de serviço (SLAs), contratos de clientes (https://aws.amazon.com/agreement/), contratos ou por meio da descrição das ofertas de serviço fornecidas on-line por meio do site da AWS. Mais informações sobre os contratos de nível de serviço podem ser encontradas em https://aws.amazon.com/legal/service-level-agreements/. Os clientes da AWS são responsáveis por: 1) Estabelecer requisitos de segurança de pessoal, incluindo funções e responsabilidades de segurança para provedores terceirizados, 2) Exigir que provedores terceirizados cumpram as políticas e procedimentos de segurança de pessoal

			avaliação, o monitoramento e o descomissionamento dos provedores de serviços. Revise e atualize a política anualmente ou quando ocorrerem mudanças corporativas significativas que possam afetar essa Salvaguarda.			estabelecidos por sua organização, 3) Documentar o pessoal requisitos de segurança, 4) Exigir que os provedores terceirizados notifiquem o pessoal ou as funções definidas pela organização de quaisquer transferências ou rescisões de pessoal de terceiros que possuam credenciais e/ou crachás organizacionais ou que tenham privilégios do sistema de informações dentro de um período de tempo definido pela organização, e 5) Monitoramento da conformidade do provedor.
Gerenciamento de provedores de serviços	15.3	Identificar	Classifique os provedores de serviços. A consideração da classificação pode incluir uma ou mais características, como a sensibilidade dos dados, o volume de dados, os requisitos de disponibilidade, as regulamentações aplicáveis, o risco inerente e o risco reduzido. Atualize e analise as classificações anualmente ou quando ocorrerem alterações corporativas significativas que possam afetar essa Salvaguarda.	AWS	Cliente	A AWS comunica compromissos de serviço a entidades de usuários (clientes da AWS) na forma de acordos de nível de serviço (SLAs), contratos de clientes (https://aws.amazon.com/agreement/), contratos ou por meio da descrição das ofertas de serviço fornecidas on-line por meio do site da AWS. Mais informações sobre os contratos de nível de serviço podem ser encontradas em https://aws.amazon.com/legal/service-level-agreements/. Os clientes da AWS são responsáveis por: 1) Estabelecer requisitos de segurança de pessoal, incluindo funções e responsabilidades de segurança para provedores terceirizados, 2) Exigir que provedores terceirizados cumpram as políticas e procedimentos de segurança de pessoal estabelecidos por sua organização, 3) Documentar o pessoal requisitos de segurança, 4) Exigir que os provedores terceirizados notifiquem o pessoal ou as funções definidas pela organização de quaisquer transferências ou rescisões de pessoal de terceiros que possuam credenciais e/ou crachás organizacionais ou que tenham privilégios do sistema de informações dentro de um período de tempo definido pela organização, e 5) Monitoramento da conformidade do provedor.

Gerenciamento de provedores de serviços	15.4	Proteger	Garantir que os contratos do provedor de serviços incluam requisitos de Os requisitos de exemplo podem incluir requisitos mínimos do programa de segurança, notificação e resposta a incidentes de segurança e/ou violação de dados, requisitos de criptografia de dados e compromissos de descarte de dados. Esses requisitos de segurança devem ser consistentes com a política de gerenciamento do provedor de serviços da empresa. Analise os contratos do provedor de serviços anualmente para garantir que os contratos não faltem requisitos de segurança.	AWS	Cliente	A AWS comunica compromissos de serviço a entidades de usuários (clientes da AWS) na forma de acordos de nível de serviço (SLAs), contratos de clientes (https://aws.amazon.com/agreement/), contratos ou por meio da descrição das ofertas de serviço fornecidas on-line por meio do site da AWS. Mais informações sobre os contratos de nível de serviço podem ser encontradas em https://aws.amazon.com/legal/service-level-agreements/. Os clientes da AWS são responsáveis por: 1) Estabelecer requisitos de segurança de pessoal, incluindo funções e responsabilidades de segurança para provedores terceirizados, 2) Exigir que provedores terceirizados cumpram as políticas e procedimentos de segurança de pessoal estabelecidos por sua organização, 3) Documentar o pessoal requisitos de segurança, 4) Exigir que os provedores terceirizados notifiquem o pessoal ou as funções definidas pela organização de quaisquer transferências ou rescisões de pessoal de terceiros que possuam credenciais e/ou crachás organizacionais ou que tenham privilégios do sistema de informações dentro de um período de tempo definido pela organização, e 5) Monitoramento da conformidade do provedor.
Gerenciamento de provedores de	15.5	Identificar	Avalie os provedores de serviços	AWS	Cliente	A AWS comunica compromissos de serviço a entidades de usuários (clientes da AWS) na forma de acordos de nível de serviço (SLAs), contratos de clientes (https://aws.amazon.com/agreement/), contratos ou por meio da descrição das ofertas de serviço fornecidas on-line por meio do site da AWS.

serviços			consistentes com a política de gerenciamento de provedores de serviços da empresa. O escopo da avaliação pode variar com base na (s) classificação (ões) e pode incluir a revisão de relatórios de avaliação padronizados, como o Service Organization Control 2 (SOC 2) e o Atestado de Conformidade (AoC) do Setor de Cartões de Pagamento (PCI), questionários personalizados ou outros processos adequadamente rigorosos. Reavalie os prestadores de serviços anualmente, no mínimo ou com contratos novos e renovados.			Mais informações sobre os contratos de nível de serviço podem ser encontradas em https://aws.amazon.com/legal/service-level-agreements/. Os clientes da AWS são responsáveis por: 1) Estabelecer requisitos de segurança de pessoal, incluindo funções e responsabilidades de segurança para provedores terceirizados, 2) Exigir que provedores terceirizados cumpram as políticas e procedimentos de segurança de pessoal estabelecidos por sua organização, 3) Documentar o pessoal requisitos de segurança, 4) Exigir que os provedores terceirizados notifiquem o pessoal ou as funções definidas pela organização de quaisquer transferências ou rescisões de pessoal de terceiros que possuam credenciais e/ou crachás organizacionais ou que tenham privilégios do sistema de informações dentro de um período de tempo definido pela organização, e 5) Monitoramento da conformidade do provedor.
Gerenciamento de provedores de serviços	15.6	Detectar	Monitore os provedores de serviços consistentes com a política de gerenciamento de provedores de	AWS	Cliente	A AWS comunica compromissos de serviço a entidades de usuários (clientes da AWS) na forma de acordos de nível de serviço (SLAs), contratos de clientes (https://aws.amazon.com/agreement/), contratos ou por meio da descrição das ofertas de serviço fornecidas on-line por meio do site da AWS. Mais informações sobre os contratos de nível de serviço podem ser encontradas em https://aws.amazon.com/legal/service-level-agreements/.

			serviços da empresa. O monitoramento pode incluir reavaliação periódica da conformidade do provedor de serviços, monitoramento de notas de versão do provedor de serviços e monitoramento da dark web.			Os clientes da AWS são responsáveis por: 1) Estabelecer requisitos de segurança de pessoal, incluindo funções e responsabilidades de segurança para provedores terceirizados, 2) Exigir que provedores terceirizados cumpram as políticas e procedimentos de segurança de pessoal estabelecidos por sua organização, 3) Documentar o pessoal requisitos de segurança, 4) Exigir que os provedores terceirizados notifiquem o pessoal ou as funções definidas pela organização de quaisquer transferências ou rescisões de pessoal de terceiros que possuam credenciais e/ou crachás organizacionais ou que tenham privilégios do sistema de informações dentro de um período de tempo definido pela organização, e 5) Monitoramento da conformidade do provedor.
Gerenciamento de provedores de serviços	15.7	Proteger	Desative os prestadores de serviços com segurança. Exemplos de considerações incluem desativação de contas de usuário e serviço, encerramento de fluxos de dados e descarte seguro de dados corporativos nos sistemas do provedor de serviços.	AWS	Cliente	A AWS comunica compromissos de serviço a entidades de usuários (clientes da AWS) na forma de acordos de nível de serviço (SLAs), contratos de clientes (https://aws.amazon.com/agreement/), contratos ou por meio da descrição das ofertas de serviço fornecidas on-line por meio do site da AWS. Mais informações sobre os contratos de nível de serviço podem ser encontradas em https://aws.amazon.com/legal/service-level-agreements/. Os clientes da AWS são responsáveis por: 1) Estabelecer requisitos de segurança de pessoal, incluindo funções e responsabilidades de segurança para provedores terceirizados, 2) Exigir que provedores terceirizados cumpram as políticas e procedimentos de segurança de pessoal estabelecidos por sua organização, 3) Documentar o pessoal requisitos de segurança, 4) Exigir que os provedores terceirizados notifiquem o pessoal ou as funções definidas pela organização de quaisquer transferências ou rescisões de pessoal de terceiros que possuam credenciais e/ou crachás organizacionais ou que tenham privilégios do sistema de informações dentro de um período de tempo definido pela organização, e 5) Monitoramento da conformidade do provedor.
Segurança de software de aplicativo	16.1	Proteger	Estabeleça e mantenha um processo seguro de desenvolvimento de aplicativos. No processo, aborde	AWS	Cliente	A AWS opera, gerencia e controla os componentes da infraestrutura, desde o sistema operacional host e a camada de virtualização até a segurança física das instalações nas quais os serviços operam. Os endpoints da AWS são testados como parte das verificações de vulnerabilidade de conformidade da AWS. Os serviços da Nuvem AWS são gerenciados de forma a preservar sua

			itens como: padrões de design de aplicativos seguros, práticas de codificação seguras, treinamento de desenvolvedores, gerenciamento de vulnerabilidades, segurança de código de terceiros e procedimentos de teste de segurança de aplicativos. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças corporativas significativas que possam afetar essa Proteção.			confidencialidade, integridade e disponibilidade. A AWS implementou procedimentos seguros de desenvolvimento de software que são seguidos para garantir que os controles de segurança apropriados sejam incorporados ao design do aplicativo. Como parte do processo de design do aplicativo, os novos aplicativos devem participar de uma análise de segurança da AWS, que inclui o registro do aplicativo, o início da classificação de risco do aplicativo, a participação na análise da arquitetura e da modelagem de ameaças, a execução da revisão do código e a execução de um teste de penetração. Os clientes da AWS são responsáveis por exigir que o desenvolvedor de seu sistema de informações, componente do sistema ou serviço do sistema de informações: 1) Execute o gerenciamento de configuração durante o projeto, desenvolvimento, implementação e/ou operação do sistema, componente ou serviço; 2) Documente, gerencie e controle a integridade de alterações nos itens de configuração definidos pela organização no gerenciamento de configuração, 3) Implementar somente alterações aprovadas pela organização no sistema, componente ou serviço, 4) Documentar alterações aprovadas no sistema, componente ou serviço e os possíveis impactos de segurança de tais alterações e 5) Controlar a segurança falhas e resolução de falhas no sistema, componente ou serviço e relate as descobertas ao pessoal definido pela organização.
Segurança de software de aplicativo	16.2	Proteger	Estabelecer e manter um processo para aceitar e tratar de relatórios de vulnerabilidades de software, incluindo o fornecimento de meios para entidades externas relatarem. O processo consiste em incluir itens como: uma política de tratamento de vulnerabilidades	AWS	Cliente	A Segurança da AWS realiza verificações regulares de vulnerabilidades no sistema operacional do host, no aplicativo da web e nos bancos de dados no ambiente da AWS usando uma variedade de ferramentas. As avaliações externas de vulnerabilidade são conduzidas por um fornecedor terceirizado aprovado pela AWS pelo menos uma vez por ano, e os problemas identificados são investigados e rastreados até a resolução. As vulnerabilidades identificadas são monitoradas e avaliadas e as contramedidas são projetadas, implementadas e operadas para compensar vulnerabilidades conhecidas e recém-identificadas. Os clientes da AWS são responsáveis por todas as verificações, testes de penetração, monitoramento de integridade de arquivos e detecção de intrusão para suas instâncias e aplicativos do Amazon EC2 e do Amazon ECS. As varreduras devem incluir endereços IP de clientes e não endpoints da AWS. Os endpoints da AWS são testados como parte das verificações de vulnerabilidade de conformidade da AWS.

			que identifica o processo de geração de relatórios, a parte responsável pelo tratamento de relatórios de vulnerabilidade e um processo para entrada, atribuição, correção e teste de correção. Como parte do processo, use um sistema de rastreamento de vulnerabilidades que inclua classificações de gravidade e métricas para medir o tempo de identificação, análise e correção de vulnerabilidades. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças corporativas significativas que possam afetar essa Proteção. Os desenvolvedores de aplicativos de terceiros precisam considerar isso como uma política voltada para o exterior que ajuda a definir			As equipes de segurança da AWS também se inscrevem em feeds de notícias sobre falhas de fornecedores aplicáveis e monitoram proativamente os sites dos fornecedores e outros veículos relevantes em busca de novos patches. Os clientes da AWS também podem relatar problemas para a AWS por meio do site de relatórios de vulnerabilidades da AWS em http://aws.amazon.com/security/vulnerability-reporting/.

			expectativas para as partes interessadas externas.			
Segurança de software de aplicativo	16.3	Proteger	Realize a análise da causa raiz das vulnerabilidades de segurança. Ao analisar vulnerabilidades, a análise de causa raiz é a tarefa de avaliar problemas subjacentes que criam vulnerabilidades no código e permite que as equipes de desenvolvimento vão além da simples correção de vulnerabilidades individuais à medida que elas surgem.	AWS	Cliente	A Segurança da AWS realiza verificações regulares de vulnerabilidades no sistema operacional do host, no aplicativo da web e nos bancos de dados no ambiente da AWS usando uma variedade de ferramentas. As avaliações externas de vulnerabilidade são conduzidas por um fornecedor terceirizado aprovado pela AWS pelo menos uma vez por ano, e os problemas identificados são investigados e rastreados até a resolução. As vulnerabilidades identificadas são monitoradas e avaliadas e as contramedidas são projetadas, implementadas e operadas para compensar vulnerabilidades conhecidas e recém-identificadas. Os clientes da AWS são responsáveis por todas as verificações, testes de penetração, monitoramento de integridade de arquivos e detecção de intrusão para suas instâncias e aplicativos do Amazon EC2 e do Amazon ECS. As varreduras devem incluir endereços IP de clientes e não endpoints da AWS. Os endpoints da AWS são testados como parte das verificações de vulnerabilidade de conformidade da AWS. As equipes de segurança da AWS também se inscrevem em feeds de notícias sobre falhas de fornecedores aplicáveis e monitoram proativamente os sites dos fornecedores e outros veículos relevantes em busca de novos patches. Os clientes da AWS também podem relatar problemas para a AWS por meio do site de relatórios de vulnerabilidades da AWS em http://aws.amazon.com/security/vulnerability-reporting/.
Segurança de software de aplicativo	16.4	Proteger	Estabelecer e gerenciar um inventário atualizado de componentes de terceiros usados no desenvolvimento, geralmente chamado de “lista de materiais”, bem como	AWS	Cliente	A AWS mantém uma abordagem sistemática para planejar e desenvolver novos serviços para o ambiente da AWS para garantir que os requisitos de qualidade e segurança sejam atendidos em cada versão. A estratégia da AWS para o projeto e desenvolvimento de serviços é definir claramente os serviços em termos de casos de uso do cliente, desempenho do serviço, requisitos de marketing e distribuição, produção e testes e requisitos legais e regulamentares. O design de todos os novos serviços ou quaisquer mudanças significativas nos serviços atuais são controlados por meio de um sistema de gerenciamento de projetos com participação multidisciplinar. Os requisitos e as especificações de serviço são estabelecidos durante o desenvolvimento do serviço, levando em consideração os requisitos legais e regulamentares, os compromissos contratuais do cliente e os requisitos para atender à

			componentes programados para uso futuro. Esse inventário deve incluir todos os riscos que cada componente de terceiros possa representar. Avalie a lista pelo menos uma vez por mês para identificar quaisquer alterações ou atualizações nesses componentes e validar se o componente ainda é suportado.			confidencialidade, integridade e disponibilidade do serviço. As análises de serviço são concluídas como parte do processo de desenvolvimento. Antes do lançamento, cada um dos seguintes requisitos deve estar completo: - Avaliação de risco de segurança - Modelagem de ameaças - Revisões de design de segurança - Revisões de código seguras - Teste de segurança - Teste de vulnerabilidade/penetração Os clientes da AWS são responsáveis por implementar um processo para controlar alterações e manter a configuração de seus sistemas. Os clientes da AWS devem realizar testes nos aplicativos que instalam, incluindo revisões de código ou testes especializados necessários antes que o software seja implantado no ambiente de produção.
Segurança de software de aplicativo	16.5	Proteger	Use componentes de software de terceiros atualizados e confiáveis. Quando possível, escolha estruturas e bibliotecas estabelecidas e comprovadas que forneçam segurança adequada. Adquira esses componentes de fontes confiáveis ou avalie o software quanto a vulnerabilidades	AWS	Cliente	A AWS mantém uma abordagem sistemática para planejar e desenvolver novos serviços para o ambiente da AWS para garantir que os requisitos de qualidade e segurança sejam atendidos em cada versão. A estratégia da AWS para o projeto e desenvolvimento de serviços é definir claramente os serviços em termos de casos de uso do cliente, desempenho do serviço, requisitos de marketing e distribuição, produção e testes e requisitos legais e regulamentares. O design de todos os novos serviços ou quaisquer mudanças significativas nos serviços atuais são controlados por meio de um sistema de gerenciamento de projetos com participação multidisciplinar. Os requisitos e as especificações de serviço são estabelecidos durante o desenvolvimento do serviço, levando em consideração os requisitos legais e regulamentares, os compromissos contratuais do cliente e os requisitos para atender à confidencialidade, integridade e disponibilidade do serviço. As análises de serviço são concluídas como parte do processo de desenvolvimento. Antes do lançamento, cada um dos seguintes requisitos deve estar completo: - Avaliação de risco de segurança

			antes de usar.			- Modelagem de ameaças - Revisões de design de segurança - Revisões de código seguras - Teste de segurança - Teste de vulnerabilidade/penetração Os clientes da AWS são responsáveis por implementar um processo para controlar alterações e manter a configuração de seus sistemas. Os clientes da AWS devem realizar testes nos aplicativos que instalam, incluindo revisões de código ou testes especializados necessários antes que o software seja implantado no ambiente de produção.
Segurança de software de aplicativo	16.6	Proteger	Estabelecer e manter um sistema e um processo de classificação de gravidade para vulnerabilidades de aplicativos que facilite a priorização da ordem em que as vulnerabilidades descobertas são corrigidas. Esse processo inclui a definição de um nível mínimo de aceitabilidade de segurança para liberar código ou aplicativos. As classificações de gravidade trazem uma maneira sistemática de triagem de vulnerabilidades	AWS	Cliente	A Segurança da AWS realiza verificações regulares de vulnerabilidades no sistema operacional do host, no aplicativo da web e nos bancos de dados no ambiente da AWS usando uma variedade de ferramentas. As avaliações externas de vulnerabilidade são conduzidas por um fornecedor terceirizado aprovado pela AWS pelo menos uma vez por ano, e os problemas identificados são investigados e rastreados até a resolução. As vulnerabilidades identificadas são monitoradas e avaliadas e as contramedidas são projetadas, implementadas e operadas para compensar vulnerabilidades conhecidas e recém-identificadas. Os clientes da AWS são responsáveis por todas as verificações, testes de penetração, monitoramento de integridade de arquivos e detecção de intrusão para suas instâncias e aplicativos do Amazon EC2 e do Amazon ECS. As varreduras devem incluir endereços IP de clientes e não endpoints da AWS. Os endpoints da AWS são testados como parte das verificações de vulnerabilidade de conformidade da AWS. As equipes de segurança da AWS também se inscrevem em feeds de notícias sobre falhas de fornecedores aplicáveis e monitoram proativamente os sites dos fornecedores e outros veículos relevantes em busca de novos patches. Os clientes da AWS também podem relatar problemas para a AWS por meio do site de relatórios de vulnerabilidades da AWS em http://aws.amazon.com/security/vulnerability-reporting/.

			que melhora o gerenciamento de riscos e ajuda a garantir que os bugs mais graves sejam corrigidos primeiro. Revise e atualize o sistema e o processo anualmente.			
Segurança de software de aplicativo	16.7	Proteger	Use modelos de configuração de proteção padrão recomendados pelo setor para componentes de infraestrutura de aplicativos. Isso inclui servidores subjacentes, bancos de dados e servidores web, e se aplica a contêineres de Cloud, componentes de Plataforma como Serviço (PaaS) e componentes SaaS. Não permita que o software desenvolvido internamente enfraqueça o endurecimento da configuração.	AWS	Cliente	As AMIs da AWS são executadas nos hipervisores Xen ou nos hipervisores Nitro — ambos são hipervisores do tipo 1 executados diretamente no hardware do servidor e nas AMIs do host. O recurso de processador Intel NX (pilha não executável) é configurado para Amazon Linux (AMI), bem como hipervisores de host (Xen e Nitro) para proteger locais de memória e criar instâncias de memória de não execução. Todos os novos hosts de hipervisor são implantados com lógica de firewall pré-instalada (que é executada no NX), uma ferramenta de gerenciamento de firewall e regras de firewall padrão. A ferramenta gerencia as regras de firewall entre o dom0 e os hosts fixos. Por padrão, o tráfego de entrada designado para o host é bloqueado e uma configuração adicional para regras de entrada é necessária para que o tráfego seja permitido. Regras de firewall adicionais exigem análise e aprovações de segurança da AWS antes de serem implantadas. Os clientes da AWS são responsáveis por configurar adequadamente suas instâncias do Amazon EC2 de acordo com as diretrizes de proteção relevantes de sua organização. Os clientes são responsáveis por proteger seus dados hospedados na AWS para evitar acesso ou divulgação não autorizados, para incluir a implementação adequada de controles de acesso, controles de fluxo de informações, criptografia, isolamento de processos e particionamento de aplicativos.
Segurança de software de aplicativo	16.8	Proteger	Manter ambientes separados para sistemas de produção e não		Cliente	Os clientes da AWS são responsáveis por desenvolver, documentar e manter sob controle de configuração uma configuração de linha de base atual de seus sistemas.

			produção.			
Segurança de software de aplicativo	16.9	Proteger	Garantir que todo o pessoal de desenvolvimento de software receba treinamento para escrever código seguro para seu ambiente de desenvolvimento e responsabilidades específicos. O treinamento pode incluir princípios gerais de segurança e práticas padrão de segurança de aplicativos. Realize treinamento pelo menos uma vez por ano e projete de forma a promover a segurança dentro da equipe de desenvolvimento e construir uma cultura de segurança entre os desenvolvedores.	AWS	Cliente	A AWS desenvolveu, documentou e disseminou conscientização sobre segurança e treinamento de segurança baseado em funções para o pessoal responsável por projetar, desenvolver, implementar, operar, manter e monitorar sistemas da AWS. O treinamento inclui, mas não está limitado a, as seguintes informações (quando relevantes para a função do funcionário): - Padrões de conduta dos trabalhadores - Procedimentos de triagem de antecedentes do - Política e procedimentos claros de mesa - Engenharia social, phishing e malware - Tratamento e proteção de dados - Compromissos de - Precauções de segurança ao viajar - Como relatar falhas de segurança e disponibilidade, incidentes, preocupações e outras reclamações ao pessoal apropriado - Como reconhecer comunicações suspeitas e comportamento anômalo em sistemas de informação organizacional - Exercícios práticos que reforçam os objetivos do treinamento - Responsabilidades do Regulamento Internacional de Tráfico de Armas (ITAR) - Planejamento de contingência - Resposta a incidentes A AWS captura e retém registros de treinamento por pelo menos cinco anos. Os clientes da AWS são responsáveis por implementar uma política e procedimentos de treinamento e conscientização de segurança para sua

						equipe, incluindo o desenvolvimento de treinamento baseado em função que atenda aos requisitos de sua organização. O cliente deve fornecer treinamento baseado em função para indivíduos atribuídos a funções e responsabilidades de segurança com o prazo definido pela organização. Além disso, o treinamento fornecido a cada indivíduo deve ser mantido conforme exigido pela organização.
Segurança de software de aplicativo	16.1	Proteger	Aplique princípios de design seguro em arquiteturas de aplicativos. Os princípios de design seguro incluem o conceito de menor privilégio e a aplicação da mediação para validar todas as operações que o usuário faz, promovendo o conceito de “nunca confie na entrada do usuário. “ Os exemplos incluem garantir que a verificação explícita de erros seja executada e documentada para todas as entradas, inclusive para tamanho, tipo de dados e intervalos ou formatos aceitáveis. O design seguro também significa minimizar a superfície de ataque à infraestrutura de aplicativos, como	AWS	Cliente	A AWS opera, gerencia e controla os componentes da infraestrutura, desde o sistema operacional do host e da camada de virtualização até a segurança física das instalações em que os serviços são executados. Os endpoints da AWS são testados como parte das verificações de vulnerabilidade de conformidade da AWS. Os serviços da Cloud AWS são gerenciados de forma a preservar sua confidencialidade, integridade e disponibilidade. A AWS implementou procedimentos seguros de desenvolvimento de software que são seguidos para garantir que os controles de segurança apropriados sejam incorporados ao design do aplicativo. Como parte do processo de design do aplicativo, os novos aplicativos devem participar de uma análise de segurança da AWS, que inclui o registro do aplicativo, o início da classificação de risco do aplicativo, a participação na análise da arquitetura e da modelagem de ameaças, a execução da revisão do código e a execução de um teste de penetração. Os clientes da AWS assumem a responsabilidade e o gerenciamento do sistema operacional convidado (incluindo atualizações e patches de segurança) e outros softwares de aplicativos associados, bem como a configuração dos firewalls de grupos de segurança fornecidos pela AWS e outros recursos de segurança, gerenciamento de alterações e registro em log. Os clientes da AWS são responsáveis por todas as verificações, monitoramento de integridade de arquivos e detecção de intrusão para suas instâncias e aplicativos do Amazon Elastic Compute Cloud (Amazon EC2).

			desativar portas e serviços desprotegidos, remover programas e arquivos desnecessários e renomear ou remover contas padrão.			
Segurança de software de aplicativo	16.11	Proteger	Aproveite os módulos ou serviços aprovados para componentes de segurança de aplicativos, como gerenciamento de identidades, criptografia, auditoria e registro em log. O uso de recursos da plataforma em funções críticas de segurança reduzirá a carga de trabalho dos desenvolvedores e minimizará a probabilidade de erros de projeto ou implementação. Os sistemas operacionais modernos fornecem mecanismos eficazes para identificação, autenticação e autorização e	AWS	Cliente	A AWS opera, gerencia e controla os componentes da infraestrutura, desde o sistema operacional do host e da camada de virtualização até a segurança física das instalações em que os serviços são executados. Os endpoints da AWS são testados como parte das verificações de vulnerabilidade de conformidade da AWS. Os serviços da Cloud AWS são gerenciados de forma a preservar sua confidencialidade, integridade e disponibilidade. A AWS implementou procedimentos seguros de desenvolvimento de software que são seguidos para garantir que os controles de segurança apropriados sejam incorporados ao design do aplicativo. Como parte do processo de design do aplicativo, os novos aplicativos devem participar de uma análise de segurança da AWS, que inclui o registro do aplicativo, o início da classificação de risco do aplicativo, a participação na análise da arquitetura e da modelagem de ameaças, a execução da revisão do código e a execução de um teste de penetração. Os clientes da AWS assumem a responsabilidade e o gerenciamento do sistema operacional convidado (incluindo atualizações e patches de segurança) e outros softwares de aplicativos associados, bem como a configuração dos firewalls de grupos de segurança fornecidos pela AWS e outros recursos de segurança, gerenciamento de alterações e registro em log. Os clientes da AWS são responsáveis por todas as verificações, monitoramento de integridade de arquivos e detecção de intrusão para suas instâncias e aplicativos do Amazon Elastic Compute Cloud (Amazon EC2).

			disponibilizam esses mecanismos para os aplicativos. Use apenas algoritmos de criptografia padronizados, atualmente aceitos e amplamente revisados. Os sistemas operacionais também fornecem mecanismos para criar e manter registros de auditoria seguros.			
Segurança de software de aplicativo	16.12	Proteger	Aplique ferramentas de análise estática e dinâmica dentro do ciclo de vida do aplicativo para verificar se as práticas de codificação segura estão sendo seguidas.	AWS	Cliente	A AWS realiza análises de segurança de aplicativos (AppSec) quando necessário para produtos, serviços e adições significativas de recursos lançados externamente antes do lançamento para garantir que os riscos de segurança sejam identificados e mitigados. Como parte da revisão do AppSec de segurança, a equipe de Segurança de Aplicativos coleta informações detalhadas sobre os artefatos necessários para a revisão. A equipe de Segurança de Aplicativos rastreia as revisões em relação a um inventário gerenciado de forma independente de produtos e recursos a serem lançados para garantir que nenhum deles seja lançado inadvertidamente antes de uma revisão concluída. Em seguida, a equipe de segurança de aplicativos determina a granularidade da análise necessária com base no design do artefato, no modelo de ameaça e no impacto no perfil de risco da AWS. Durante esse processo, eles trabalham com a equipe de serviço para identificar, priorizar e corrigir descobertas de segurança e realizar testes de penetração conforme necessário. A equipe de Segurança de Aplicativos fornece sua aprovação final para o lançamento somente após a conclusão da revisão. Os clientes da AWS são responsáveis por implementar um processo de controle de alterações de configuração de acordo com sua política de gerenciamento de configuração que inclui os seguintes elementos: 1) Determinação dos tipos de alterações no sistema de informações que são controladas pela configuração, 2) Revisão de todas as propostas alterações controladas pela configuração no sistema de informação e aprovação ou reprovação de tais alterações com consideração explícita para análises de

						impacto na segurança, 3) Documentação das decisões de alteração de configuração associadas ao sistema de informação, 4) Implementação de alterações controladas pela configuração aprovadas para o sistema de informações, 5) Retenção de registros de alterações controladas por configuração no sistema de informações por um período de tempo definido pela organização.
Segurança de software de aplicativo	16.13	Proteger	Realize testes de penetração de aplicativos. Para aplicativos críticos, o teste de penetração autenticado é mais adequado para encontrar vulnerabilidades de lógica de negócios do que a verificação de código e os testes de segurança automatizados. O teste de penetração depende da habilidade do testador para manipular manualmente um aplicativo como um usuário autenticado e não autenticado.		Cliente	Os clientes da AWS são responsáveis por realizar a verificação de vulnerabilidades e testes de penetração de seus sistemas hospedados na AWS e por corrigir quaisquer vulnerabilidades descobertas. Os clientes devem enviar uma notificação à AWS antes de realizar testes de vulnerabilidade por meio do site da AWS em https://aws.amazon.com/security/penetration-testing/. Além da verificação de vulnerabilidades, os clientes da AWS são responsáveis por receber e disseminar alertas e recomendações de segurança, conforme necessário, para facilitar as atividades contínuas de gerenciamento de patches.
Segurança de software de aplicativo	16.14	Proteger	Conduza modelos de ameaças. A modelagem de ameaças é o processo de identificar e resolver falhas de	AWS	Cliente	A AWS realiza análises de segurança de aplicativos (AppSec) quando necessário para produtos, serviços e adições significativas de recursos lançados externamente antes do lançamento para garantir que os riscos de segurança sejam identificados e mitigados. Como parte da revisão do AppSec de segurança, a equipe de Segurança de Aplicativos coleta informações detalhadas sobre os artefatos necessários para a revisão. A equipe de Segurança de Aplicativos rastreia as revisões em relação a um inventário gerenciado de forma independente de produtos e recursos a serem lançados

			design de segurança de aplicativos dentro de um design, antes que o código seja criado. É conduzido por indivíduos especialmente treinados que avaliam o design do aplicativo e avaliam os riscos de segurança para cada ponto de entrada e nível de acesso. O objetivo é mapear o aplicativo, a arquitetura e a infraestrutura de forma estruturada para entender seus pontos fracos.			para garantir que nenhum deles seja lançado inadvertidamente antes de uma revisão concluída. Em seguida, a equipe de segurança de aplicativos determina a granularidade da análise necessária com base no design do artefato, no modelo de ameaça e no impacto no perfil de risco da AWS. Durante esse processo, eles trabalham com a equipe de serviço para identificar, priorizar e corrigir descobertas de segurança e realizar testes de penetração conforme necessário. A equipe de Segurança de Aplicativos fornece sua aprovação final para o lançamento somente após a conclusão da revisão. Os clientes da AWS são responsáveis por implementar um processo de controle de alterações de configuração de acordo com sua política de gerenciamento de configuração que inclui os seguintes elementos: 1) Determinação dos tipos de alterações no sistema de informações que são controladas pela configuração, 2) Revisão de todas as propostas alterações controladas pela configuração no sistema de informação e aprovação ou reprovação de tais alterações com consideração explícita para análises de impacto na segurança, 3) Documentação das decisões de alteração de configuração associadas ao sistema de informação, 4) Implementação de alterações controladas pela configuração aprovadas para o sistema de informações, 5) Retenção de registros de alterações controladas por configuração no sistema de informações por um período de tempo definido pela organização.
Gerenciamento de resposta a incidentes	17.1	Responder	Designe uma pessoa-chave e pelo menos um backup que gerenciará o processo de tratamento de incidentes da empresa. A equipe de gerenciamento é responsável pela coordenação e documentação dos esforços de resposta e recuperação de incidentes e pode	AWS	Cliente	A AWS mantém políticas formais que fornecem orientação para a segurança das informações dentro da organização e do ambiente de TI de suporte. A Segurança da AWS estabelece e mantém políticas e procedimentos para delinear padrões de acesso lógico no sistema e nos hosts de infraestrutura da AWS. As políticas também identificam as responsabilidades funcionais pela administração do acesso lógico e da segurança. Quando aplicável, a Segurança da AWS aproveita a estrutura e as políticas do sistema de informações estabelecidas e mantidas pelo Amazon Corporate Information Security. As políticas de segurança de informações corporativas da AWS e da Amazon são revisadas e aprovadas anualmente pela liderança de segurança da AWS e são usadas para apoiar a AWS no cumprimento dos compromissos de serviço assumidos ao cliente. Os clientes mantêm o controle e são responsáveis por seus dados, controles de segurança e procedimentos. Como os clientes mantêm o controle de seu conteúdo ao usar a AWS, os clientes mantêm a responsabilidade de monitorar seu próprio ambiente em busca de violações de privacidade e notificar os

			consistir em funcionários internos da empresa, fornecedores terceirizados ou uma abordagem híbrida. Se estiver usando um fornecedor terceirizado, designe pelo menos uma pessoa interna da empresa para supervisionar qualquer trabalho de terceiros. Analise anualmente ou quando ocorrerem mudanças corporativas significativas que possam afetar essa proteção.			reguladores e os indivíduos afetados, conforme exigido pela lei aplicável. Somente o cliente é capaz de gerenciar essa responsabilidade.
Gerenciamento de resposta a incidentes	17.2	Responder	Estabelecer e manter informações de contato para as partes que precisam ser informadas sobre incidentes de segurança. Os contatos podem incluir funcionários internos, fornecedores terceirizados, agentes da lei, provedores de	AWS	Cliente	A AWS mantém políticas formais que fornecem orientação para a segurança das informações dentro da organização e do ambiente de TI de suporte. A Segurança da AWS estabelece e mantém políticas e procedimentos para delinear padrões de acesso lógico no sistema e nos hosts de infraestrutura da AWS. As políticas também identificam as responsabilidades funcionais pela administração do acesso lógico e da segurança. Quando aplicável, a Segurança da AWS aproveita a estrutura e as políticas do sistema de informações estabelecidas e mantidas pelo Amazon Corporate Information Security. As políticas de segurança de informações corporativas da AWS e da Amazon são revisadas e aprovadas anualmente pela liderança de segurança da AWS e são usadas para apoiar a AWS no cumprimento dos compromissos de serviço assumidos ao cliente. Os clientes mantêm o controle e são responsáveis por seus dados, controles de segurança e procedimentos. Como os clientes mantêm o controle de seu conteúdo ao usar a AWS, os clientes mantêm a responsabilidade de monitorar

			seguros cibernéticos, agências governamentais relevantes, parceiros do Centro de Análise e Compartilhamento de Informações (ISAC) ou outras partes interessadas. Verifique os contatos anualmente para garantir que as informações estejam atualizadas.			seu próprio ambiente em busca de violações de privacidade e notificar os reguladores e os indivíduos afetados, conforme exigido pela lei aplicável. Somente o cliente é capaz de gerenciar essa responsabilidade.
Gerenciamento de resposta a incidentes	17.3	Responder	Estabelecer e manter um processo corporativo para a força de trabalho relatar incidentes de segurança. O processo inclui cronograma de relatório, pessoal a ser reportado, mecanismo de relatório e as informações mínimas a serem relatadas. Garanta que o processo esteja disponível publicamente para toda a força de trabalho. Analise anualmente ou	AWS	Cliente	A AWS mantém políticas formais que fornecem orientação para a segurança das informações dentro da organização e do ambiente de TI de suporte. A Segurança da AWS estabelece e mantém políticas e procedimentos para delinear padrões de acesso lógico no sistema e nos hosts de infraestrutura da AWS. As políticas também identificam as responsabilidades funcionais pela administração do acesso lógico e da segurança. Quando aplicável, a Segurança da AWS aproveita a estrutura e as políticas do sistema de informações estabelecidas e mantidas pelo Amazon Corporate Information Security. As políticas de segurança de informações corporativas da AWS e da Amazon são revisadas e aprovadas anualmente pela liderança de segurança da AWS e são usadas para apoiar a AWS no cumprimento dos compromissos de serviço assumidos ao cliente. Os clientes mantêm o controle e são responsáveis por seus dados, controles de segurança e procedimentos. Como os clientes mantêm o controle de seu conteúdo ao usar a AWS, os clientes mantêm a responsabilidade de monitorar seu próprio ambiente em busca de violações de privacidade e notificar os reguladores e os indivíduos afetados, conforme exigido pela lei aplicável. Somente o cliente é capaz de gerenciar essa responsabilidade.

			quando ocorrerem mudanças corporativas significativas que possam afetar essa proteção.			
Gerenciamento de resposta a incidentes	17.4	Responder	Estabelecer e manter um processo de resposta a incidentes que trate de funções e responsabilidades, requisitos de conformidade e um plano de comunicação. Analise anualmente ou quando ocorrerem mudanças corporativas significativas que possam afetar essa proteção.	AWS	Cliente	A AWS mantém políticas formais que fornecem orientação para a segurança das informações dentro da organização e do ambiente de TI de suporte. A Segurança da AWS estabelece e mantém políticas e procedimentos para delinear padrões de acesso lógico no sistema e nos hosts de infraestrutura da AWS. As políticas também identificam as responsabilidades funcionais pela administração do acesso lógico e da segurança. Quando aplicável, a Segurança da AWS aproveita a estrutura e as políticas do sistema de informações estabelecidas e mantidas pelo Amazon Corporate Information Security. As políticas de segurança de informações corporativas da AWS e da Amazon são revisadas e aprovadas anualmente pela liderança de segurança da AWS e são usadas para apoiar a AWS no cumprimento dos compromissos de serviço assumidos ao cliente. Os clientes mantêm o controle e são responsáveis por seus dados, controles de segurança e procedimentos. Como os clientes mantêm o controle de seu conteúdo ao usar a AWS, os clientes mantêm a responsabilidade de monitorar seu próprio ambiente em busca de violações de privacidade e notificar os reguladores e os indivíduos afetados, conforme exigido pela lei aplicável. Somente o cliente é capaz de gerenciar essa responsabilidade.
Gerenciamento de resposta a incidentes	17.5	Responder	Atribua as principais funções e responsabilidades para a resposta a incidentes, incluindo equipes jurídicas, de TI, segurança da informação, instalações, relações públicas, recursos humanos, respondentes a incidentes e	AWS	Cliente	A AWS mantém políticas formais que fornecem orientação para a segurança das informações dentro da organização e do ambiente de TI de suporte. A Segurança da AWS estabelece e mantém políticas e procedimentos para delinear padrões de acesso lógico no sistema e nos hosts de infraestrutura da AWS. As políticas também identificam as responsabilidades funcionais pela administração do acesso lógico e da segurança. Quando aplicável, a Segurança da AWS aproveita a estrutura e as políticas do sistema de informações estabelecidas e mantidas pelo Amazon Corporate Information Security. As políticas de segurança de informações corporativas da AWS e da Amazon são revisadas e aprovadas anualmente pela liderança de segurança da AWS e são usadas para apoiar a AWS no cumprimento dos compromissos de serviço assumidos ao cliente. Os clientes mantêm o controle e são responsáveis por seus dados, controles de segurança e procedimentos. Como os clientes mantêm o controle de seu

			analistas, conforme aplicável. Analise anualmente ou quando ocorrerem mudanças corporativas significativas que possam afetar essa proteção.			conteúdo ao usar a AWS, os clientes mantêm a responsabilidade de monitorar seu próprio ambiente em busca de violações de privacidade e notificar os reguladores e os indivíduos afetados, conforme exigido pela lei aplicável. Somente o cliente é capaz de gerenciar essa responsabilidade.
Gerenciamento de resposta a incidentes	17.6	Responder	Determine quais mecanismos primários e secundários serão usados para se comunicar e relatar durante um incidente de segurança. Os mecanismos podem incluir chamadas telefônicas, e-mails ou cartas. Lembre-se de que certos mecanismos, como e-mails, podem ser afetados durante um incidente de segurança. Analise anualmente ou quando ocorrerem mudanças corporativas significativas que possam afetar essa proteção.	AWS	Cliente	Os clientes podem manter uma variedade de registros e automatizar as notificações. A AWS oferece serviços como o Amazon CloudWatch para monitorar os recursos da Cloud da AWS e os aplicativos que você executa na AWS. Os clientes podem usar o Amazon CloudWatch para coletar e rastrear métricas, coletar e monitorar arquivos de log, definir alarmes, enviar notificações e reagir automaticamente a alterações em seus recursos da AWS. Com o AWS CloudTrail, você pode registrar, monitorar continuamente e reter eventos relacionados a chamadas de interface de programação de aplicativos (API) em toda a infraestrutura da AWS. Para obter mais informações sobre registro e monitoramento, visite https://docs.aws.amazon.com/whitepapers/latest/aws-security-best-practices/. A AWS implementou uma política formal e documentada de resposta a incidentes e um programa desenvolvidos em alinhamento com os padrões ISO 27001.
Gerenciament	17.7	Recuperar	Planeje e conduza	AWS	Cliente	Os manuais de planejamento de contingência e resposta a incidentes da AWS

o de resposta a incidentes			exercícios e cenários de resposta a incidentes de rotina para o pessoal-chave envolvido no processo de resposta a incidentes, a fim de se preparar para responder a incidentes do mundo real. Os exercícios precisam testar canais de comunicação, tomada de decisões e fluxos de trabalho. Realize testes anualmente, no mínimo.			são mantidos e atualizados para refletir os riscos emergentes de continuidade e as lições aprendidas com incidentes anteriores. O plano de contingência da AWS é testado pelo menos uma vez por ano. Os planos de resposta da equipe de serviço são testados e atualizados durante o curso adequado dos negócios, e o plano de resiliência da AWS é testado, revisado e aprovado pela liderança sênior anualmente. Os clientes mantêm o controle e são responsáveis por seus dados, controles de segurança e procedimentos. Como os clientes mantêm o controle de seu conteúdo ao usar a AWS, os clientes mantêm a responsabilidade de monitorar seu próprio ambiente em busca de violações de privacidade e notificar os reguladores e os indivíduos afetados, conforme exigido pela lei aplicável. Somente o cliente é capaz de gerenciar essa responsabilidade.
Gerenciamento de resposta a incidentes	17.8	Recuperar	Realizar análises pós-incidentes. As revisões pós-incidentes ajudam a evitar a recorrência de incidentes por meio da identificação das lições aprendidas e das ações	AWS	Cliente	Os incidentes são registrados em um sistema de emissão de tíquetes, atribuídos a classificação de gravidade e rastreados até a resolução. A equipe de segurança da AWS é responsável por monitorar sistemas, rastrear problemas e documentar descobertas de eventos relacionados à segurança. Os registros são mantidos para praias de segurança e incidentes, o que inclui informações de status, informações necessárias para apoiar atividades forenses, análise de tendências e avaliação de detalhes do incidente. A documentação é mantida para ajudar e informar o pessoal de operações no tratamento de incidentes ou problemas. Se a resolução de um problema exigir colaboração, será usado um sistema de emissão de tíquetes que suporta comunicação, atualizações de progresso e recursos de registro. Líderes de chamada treinados facilitam a comunicação e o progresso durante o tratamento de problemas operacionais que exigem colaboração. Depois que as revisões de ação são convocadas após qualquer problema operacional significativo, independentemente do impacto externo, e os documentos de Correção de Erros (COE) são compostos de forma que a causa raiz seja capturada e ações preventivas possam ser tomadas para o futuro. A implementação das medidas preventivas identificadas nos COEs é rastreada

						durante as reuniões semanais de operações. Os clientes mantêm o controle e são responsáveis por seus dados, controles de segurança e procedimentos. Como os clientes mantêm o controle de seu conteúdo ao usar a AWS, os clientes mantêm a responsabilidade de monitorar seu próprio ambiente em busca de violações de privacidade e notificar os reguladores e os indivíduos afetados, conforme exigido pela lei aplicável. Somente o cliente é capaz de gerenciar essa responsabilidade.
Gerenciamento de resposta a incidentes	17.9	Recuperar	Estabeleça e mantenha limites de incidentes de segurança, incluindo, no mínimo, a diferenciação entre um incidente e um evento. Os exemplos podem incluir: atividade anormal, vulnerabilidade de segurança, fraqueza de segurança, violação de dados, incidente de privacidade, etc. Analise anualmente ou quando ocorrerem mudanças corporativas significativas que possam afetar essa proteção.	AWS	Cliente	Os incidentes são registrados em um sistema de emissão de tíquetes, atribuídos a classificação de gravidade e rastreados até a resolução. Os incidentes são registrados em um sistema de emissão de tíquetes, atribuídos a classificação de gravidade e rastreados até a resolução. A equipe de segurança da AWS é responsável por monitorar sistemas, rastrear problemas e documentar descobertas de eventos relacionados à segurança. Os registros são mantidos para praias de segurança e incidentes, o que inclui informações de status, informações necessárias para apoiar atividades forenses, análise de tendências e avaliação de detalhes do incidente. A documentação é mantida para ajudar e informar o pessoal de operações no tratamento de incidentes ou problemas. Se a resolução de um problema exigir colaboração, será usado um sistema de emissão de tíquetes que suporta comunicação, atualizações de progresso e recursos de registro. Líderes de chamada treinados facilitam a comunicação e o progresso durante o tratamento de problemas operacionais que exigem colaboração. Depois que as revisões de ação são convocadas após qualquer problema operacional significativo, independentemente do impacto externo, e os documentos de Correção de Erros (COE) são compostos de forma que a causa raiz seja capturada e ações preventivas possam ser tomadas para o futuro. A implementação das medidas preventivas identificadas nos COEs é rastreada durante as reuniões semanais de operações. Os clientes mantêm o controle e são responsáveis por seus dados, controles de segurança e procedimentos. Como os clientes mantêm o controle de seu conteúdo ao usar a AWS, os clientes mantêm a responsabilidade de monitorar seu próprio ambiente em busca de violações de privacidade e notificar os reguladores e os indivíduos afetados, conforme exigido pela lei aplicável. Somente o cliente é capaz de gerenciar essa responsabilidade.
Testes de invasão	18.1	Identificar	Estabelecer e manter um	AWS	Cliente	A AWS mantém políticas formais que fornecem orientação para a segurança das informações dentro da organização e do ambiente de TI de suporte. A

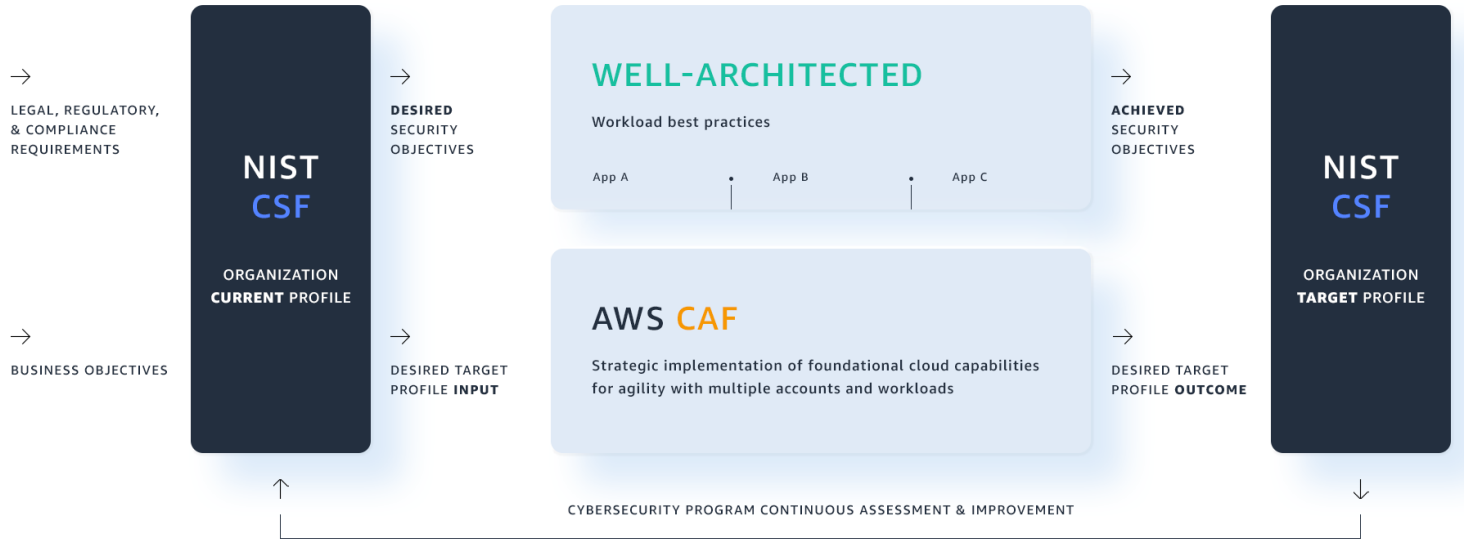
			programa de teste de penetração adequado ao tamanho, complexidade e maturidade da empresa. As características do programa de teste de penetração incluem escopo, como rede, aplicativo da web, interface de programação de aplicativos (API), serviços hospedados e controles físicos de premissa; frequência; limitações, como horas aceitáveis e tipos de ataque excluídos; informações de ponto de contato; remediação, como como os resultados serão encaminhados internamente; e os requisitos retrospectivos.			Segurança da AWS estabelece e mantém políticas e procedimentos para delinear padrões de acesso lógico no sistema e nos hosts de infraestrutura da AWS. As políticas também identificam as responsabilidades funcionais pela administração do acesso lógico e da segurança. Quando aplicável, a Segurança da AWS aproveita a estrutura e as políticas do sistema de informações estabelecidas e mantidas pelo Amazon Corporate Information Security. As políticas de segurança de informações corporativas da AWS e da Amazon são revisadas e aprovadas anualmente pela liderança de segurança da AWS e são usadas para apoiar a AWS no cumprimento dos compromissos de serviço assumidos ao cliente. Os clientes da AWS podem realizar avaliações de segurança ou testes de penetração em sua infraestrutura da AWS sem aprovação prévia para os serviços listados. A solicitação de autorização para outros eventos simulados deve ser enviada por meio do formulário Eventos simulados.
Testes de invasão	18.2	Identificar	Realize testes periódicos de penetração externa com base nos requisitos do programa, não menos que anualmente. Os	AWS	Cliente	A AWS mantém políticas formais que fornecem orientação para a segurança das informações dentro da organização e do ambiente de TI de suporte. A Segurança da AWS estabelece e mantém políticas e procedimentos para delinear padrões de acesso lógico no sistema e nos hosts de infraestrutura da AWS. As políticas também identificam as responsabilidades funcionais pela administração do acesso lógico e da segurança. Quando aplicável, a Segurança da AWS aproveita a estrutura e as políticas do sistema de informações estabelecidas e mantidas pelo Amazon Corporate Information

			testes de penetração externa devem incluir reconhecimento corporativo e ambiental para detectar informações exploráveis. O teste de penetração requer habilidades e experiência especializadas e deve ser conduzido por meio de uma parte qualificada. O teste pode ser caixa transparente ou caixa opaca.			Security. As políticas de segurança de informações corporativas da AWS e da Amazon são revisadas e aprovadas anualmente pela liderança de segurança da AWS e são usadas para apoiar a AWS no cumprimento dos compromissos de serviço assumidos ao cliente. Os clientes da AWS podem realizar avaliações de segurança ou testes de penetração em sua infraestrutura da AWS sem aprovação prévia para os serviços listados. A solicitação de autorização para outros eventos simulados deve ser enviada por meio do formulário Eventos simulados.
Testes de invasão	18.3	Proteger	Corrija as descobertas do teste de penetração com base na política da empresa para o escopo e a priorização da remediação.	AWS	Cliente	A AWS mantém políticas formais que fornecem orientação para a segurança das informações dentro da organização e do ambiente de TI de suporte. A Segurança da AWS estabelece e mantém políticas e procedimentos para delinear padrões de acesso lógico no sistema e nos hosts de infraestrutura da AWS. As políticas também identificam as responsabilidades funcionais pela administração do acesso lógico e da segurança. Quando aplicável, a Segurança da AWS aproveita a estrutura e as políticas do sistema de informações estabelecidas e mantidas pelo Amazon Corporate Information Security. As políticas de segurança de informações corporativas da AWS e da Amazon são revisadas e aprovadas anualmente pela liderança de segurança da AWS e são usadas para apoiar a AWS no cumprimento dos compromissos de serviço assumidos ao cliente. Os clientes da AWS podem realizar avaliações de segurança ou testes de penetração em sua infraestrutura da AWS sem aprovação prévia para os serviços listados. A solicitação de autorização para outros eventos simulados deve ser enviada por meio do formulário Eventos simulados.
Testes de	18.4	Proteger	Valide as medidas	AWS	Cliente	A AWS mantém políticas formais que fornecem orientação para a segurança

invasão			de segurança após cada teste de penetração. Se for considerado necessário, modifique os conjuntos de regras e os recursos para detectar as técnicas usadas durante o teste.			das informações dentro da organização e do ambiente de TI de suporte. A Segurança da AWS estabelece e mantém políticas e procedimentos para delinear padrões de acesso lógico no sistema e nos hosts de infraestrutura da AWS. As políticas também identificam as responsabilidades funcionais pela administração do acesso lógico e da segurança. Quando aplicável, a Segurança da AWS aproveita a estrutura e as políticas do sistema de informações estabelecidas e mantidas pelo Amazon Corporate Information Security. As políticas de segurança de informações corporativas da AWS e da Amazon são revisadas e aprovadas anualmente pela liderança de segurança da AWS e são usadas para apoiar a AWS no cumprimento dos compromissos de serviço assumidos ao cliente. Os clientes da AWS podem realizar avaliações de segurança ou testes de penetração em sua infraestrutura da AWS sem aprovação prévia para os serviços listados. A solicitação de autorização para outros eventos simulados deve ser enviada por meio do formulário Eventos simulados.
Testes de invasão	18.5	Identificar	Realize testes periódicos de penetração interna com base nos requisitos do programa, não menos que anualmente. O teste pode ser caixa transparente ou caixa opaca.	AWS	Cliente	A AWS mantém políticas formais que fornecem orientação para a segurança das informações dentro da organização e do ambiente de TI de suporte. A Segurança da AWS estabelece e mantém políticas e procedimentos para delinear padrões de acesso lógico no sistema e nos hosts de infraestrutura da AWS. As políticas também identificam as responsabilidades funcionais pela administração do acesso lógico e da segurança. Quando aplicável, a Segurança da AWS aproveita a estrutura e as políticas do sistema de informações estabelecidas e mantidas pelo Amazon Corporate Information Security. As políticas de segurança de informações corporativas da AWS e da Amazon são revisadas e aprovadas anualmente pela liderança de segurança da AWS e são usadas para apoiar a AWS no cumprimento dos compromissos de serviço assumidos ao cliente. Os clientes da AWS podem realizar avaliações de segurança ou testes de penetração em sua infraestrutura da AWS sem aprovação prévia para os serviços listados. A solicitação de autorização para outros eventos simulados deve ser enviada por meio do formulário Eventos simulados.

Frameworks Adicionais Recomendados

Para complementar os controles CIS apresentados acima e as medidas de segurança que podem ajudar os clientes a alcançar a conformidade com as “Práticas recomendadas de segurança” do Capítulo VII da LGPD, muitos clientes estabelecem uma base de segurança usando estruturas de gerenciamento de risco independentes de tecnologia, como o National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) — para entender os recursos atuais de sua organização, definir metas e desenvolver um plano para melhorar e manter a postura de segurança. No entanto, você ainda precisa do modelo certo para otimizar os resultados de segurança na nuvem. Para ajudá-lo a adaptar seu programa de segurança para a nuvem, a AWS desenvolveu duas ferramentas: AWS Cloud Adoption Framework (CAF) e AWS Well-Architected Framework. Complementando sua base baseada em riscos com o AWS CAF, você pode integrar seus direcionadores de negócios organizacionais em escala à medida que migra para a nuvem; e, quando estiver pronto para implementar cargas de trabalho específicas, poderá usar o AWS Well-Architected Framework para projetar, medir e aprimorar suas informações técnicas implementação.



Usando o NIST CSF, o AWS CAF e o AWS Well-Architected, você pode personalizar sua abordagem para incorporar as melhores práticas de gerenciamento de segurança para sua jornada na nuvem. Essas três estruturas oferecem lentes relacionadas, mas distintas, sobre como abordar a segurança da sua organização, conectando metas e resultados de negócios ao seu programa de segurança.

Usando o NIST CSF, você pode desenvolver um entendimento organizacional para gerenciar riscos de segurança. Usando o AWS CAF, você pode planejar sua abordagem de segurança na nuvem e mapear atividades para controles de segurança que operam na nuvem e escalá-los em toda a organização. Isso ajudará você a construir sua arquitetura. Você pode usar o AWS Well-Architected para medir consistentemente sua carga de trabalho em relação às melhores práticas e identificar áreas de melhoria.

Abaixo estão algumas recomendações para ajudá-lo a aproveitar esse novo entendimento e orientá-lo pelas diferentes estruturas que podem ajudá-lo a atingir seus objetivos de segurança e conformidade:

- Recursos:
    - Alinhamento ao NIST Cybersecurity Framework na Nuvem AWS white paper e workbook associado
    - AWS Cloud Adoption Framework, especificamente a Perspectiva de Segurança
    - AWS AWS Well-Architected Framework, especificamente os pilares de Segurança e Confiabilidade
    - Documentação de serviços da AWS para os serviços que você está usando ou considera usar
- Use a ferramenta AWS Well-Architected para realizar uma autoavaliação do seu alinhamento com as melhores práticas da AWS.

A tabela a seguir mapeia as cinco funções do Framework de Privacidade do NIST (PF) e suas categorias para as seis perspectivas do AWS CAF e seus recursos. O NIST PF também pode mapear o NIST CSF e ajudar as empresas com seus controles de privacidade que suportam os requisitos da LGPD.

Framework de Privacidade do NIST	**AWS CAF**
Categorias NIST Identificar-P	**Recursos de perspectiva de negócios do AWS CAF**
Inventário e mapeamento (ID.IM-P)	**Finanças de TI**
O processamento de dados por sistemas, produtos ou serviços é entendido e informa o gerenciamento dos riscos de privacidade. Ambiente de negócios **(ID.BE-P)**	Aborda sua capacidade de planejar, alocar e gerenciar o orçamento para despesas de TI com o modelo de custo baseado no uso dos serviços em nuvem.
A missão, os objetivos, as partes interessadas e as atividades da organização são compreendidas e priorizadas. Essas informações são usadas para informar as funções de privacidade, responsabilidades e decisões de gerenciamento de riscos. Avaliação de risco **(ID.RA-P)**	Estratégia de TI ajuda você a aproveitar a abordagem de TI baseada em nuvem para oferecer valor e adoção pelo usuário final. Realização de benefícios
A organização entende os riscos de privacidade para os indivíduos e como esses riscos de privacidade podem criar impactos subsequentes nas operações organizacionais, incluindo missão, funções, outras prioridades de gerenciamento de riscos (por exemplo, conformidade, finanças), reputação, força de trabalho e cultura.	Ajuda você a medir os benefícios de seus investimentos em TI usando métodos para um modelo operacional de TI baseado em nuvem.

Gerenciamento de riscos do ecossistema de processamento de dados (ID.DE-P)	Gestão de riscos de negócios
As prioridades, restrições, tolerância ao risco e suposições da organização são estabelecidas e usadas para apoiar decisões de risco associadas ao gerenciamento de riscos de privacidade e terceiros dentro do ecossistema de processamento de dados.	Ajuda a estimar o possível impacto comercial de riscos evitáveis, estratégicos e/ou externos.
Categorias NIST Governar-P (GV-P)	**Recursos de perspectiva de pessoas do AWS CAF**
Políticas, processos e procedimentos de governança (GV.PO-P)	**Gestão de incentivos**
As políticas, processos e procedimentos para gerenciar e monitorar os requisitos regulatórios, legais, de risco, ambientais e operacionais da organização são compreendidos e informam o gerenciamento do risco de privacidade. Estratégia de gerenciamento de riscos **(GV.RM-P)**	Ajuda a implementar um programa de remuneração que atrairá e reterá o pessoal necessário para operar um modelo de TI baseado em nuvem. Gerenciamento de treinamento
As prioridades, restrições, tolerâncias de risco e suposições da organização são estabelecidas e usadas para apoiar decisões de risco operacional. Conscientização e treinamento **(GV.AT-P)**	
A força de trabalho da organização e os terceiros envolvidos no processamento de dados recebem educação sobre conscientização sobre privacidade e são treinados para desempenhar seus deveres e responsabilidades relacionados à privacidade de acordo com as políticas, processos, procedimentos e acordos relacionados e valores de privacidade organizacional.	Fornece orientação sobre como desenvolver ou adquirir treinamento para seus funcionários para que eles possam desempenhar suas funções em um ambiente de nuvem.
Monitoramento e revisão (GV.MT-P)	
As políticas, processos e procedimentos para a revisão contínua da postura de privacidade da organização são compreendidos e informam o gerenciamento do risco de privacidade.	

Categorias NIST Comunicação-P (CM-P)	Recursos de perspectiva de pessoas do AWS CAF
Políticas, processos e procedimentos de comunicação (CM.PO-P)	**Gerenciamento de recursos**
Políticas, processos e procedimentos são mantidos e usados para aumentar a transparência das práticas de processamento de dados da organização (por exemplo, finalidade, escopo, funções e responsabilidades no ecossistema de processamento de dados e compromisso de gerenciamento) e riscos de privacidade associados. Consciência de processamento de dados **(CM.AW-P)**	Ajuda você a entender e prever novas necessidades de pessoal para um modelo baseado em nuvem. Gestão de carreira
Indivíduos e organizações têm conhecimento confiável sobre práticas de processamento de dados e riscos de privacidade associados, e mecanismos eficazes são usados e mantidos para aumentar a previsibilidade consistente com a estratégia de risco da organização para proteger a privacidade dos indivíduos.	Ajuda você a identificar, adquirir e reter as habilidades necessárias para a migração para a nuvem e o modelo operacional contínuo. Gestão de mudanças organizacionais
	Ajuda a gerenciar o impacto das mudanças comerciais, estruturais e culturais causadas pela adoção da nuvem.
Categorias NIST Governar-P (GV-P)	**Recursos de perspectiva de governança da AWS CAF**
Políticas, processos e procedimentos de governança (GV.PO-P)	**Gerenciamento de portfólio**
As políticas, processos e procedimentos para gerenciar e monitorar os requisitos regulatórios, legais, de risco, ambientais e operacionais da organização são compreendidos e informam o gerenciamento do risco de privacidade. Estratégia de gerenciamento de riscos **(GV.RM-P)**	Fornece um mecanismo para gerenciá-lo com base nos resultados comerciais desejados. Isso pode ajudar a determinar a elegibilidade da nuvem para cargas de trabalho ao priorizar quais serviços devem ser movidos para a nuvem. Gerenciamento de programas e projetos
As prioridades, restrições, tolerâncias de risco e suposições da organização são estabelecidas e usadas para apoiar decisões de risco operacional. Conscientização e treinamento (GV.AT-P)	Ajuda a gerenciar projetos de tecnologia usando metodologias que aproveitam os benefícios da agilidade e do gerenciamento de custos inerentes aos serviços em nuvem. Medição de desempenho empresarial

A força de trabalho da organização e os terceiros envolvidos no processamento de dados recebem educação sobre conscientização sobre privacidade e são treinados para desempenhar seus deveres e responsabilidades relacionados à privacidade de acordo com as políticas, processos, procedimentos e acordos relacionados e valores de privacidade organizacional.	Ajuda a medir o impacto da nuvem nos objetivos de negócios.
Monitoramento e revisão (GV.MT-P)	**Gerenciamento de licenças**
As políticas, processos e procedimentos para a revisão contínua da postura de privacidade da organização são compreendidos e informam o gerenciamento do risco de privacidade.	Define métodos para adquirir, distribuir e gerenciar as licenças necessárias para sistemas, serviços e software de TI.
Categorias NIST Controle-P (CT-P)	**Recursos de perspectiva da plataforma AWS CAF**
Políticas, processos e procedimentos de processamento de dados (CT.PO-P)	**Arquitetura de sistemas e soluções**
Políticas, processos e procedimentos são mantidos e usados para gerenciar o processamento de dados (por exemplo, finalidade, escopo, funções e responsabilidades no ecossistema de processamento de dados e compromisso de gerenciamento) consistente com a estratégia de risco da organização para proteger a privacidade dos indivíduos. Gerenciamento de processamento de dados **(CT.DM-P)**	Auxilia você a definir e descrever o design do sistema e seus padrões arquitetônicos. Provisionamento de computação, rede, armazenamento e banco de dados
Os dados são gerenciados de acordo com a estratégia de risco da organização para proteger a privacidade dos indivíduos, aumentar a capacidade de gerenciamento e permitir a implementação de princípios de privacidade (por exemplo, participação individual, qualidade dos dados, minimização de dados) .Processamento desassociado **(CT.DP-P)**	Ajuda a desenvolver novos processos para provisionamento de infraestrutura em um ambiente de nuvem. O provisionamento muda de um foco operacional alinhando a oferta com a demanda, para um foco arquitetônico que alinha os serviços aos requisitos. Desenvolvimento de aplicativos

As soluções de processamento de dados aumentam a desassociabilidade consistente com a estratégia de risco da organização para proteger a privacidade dos indivíduos e permitir a implementação de princípios de privacidade (por exemplo, minimização de dados).	Aborda sua capacidade de apoiar metas de negócios com aplicativos novos ou atualizados e ajuda a implementar novas habilidades e processos para o desenvolvimento de software que aproveitam a agilidade obtida pela computação em nuvem.
Proteção de dados, políticas, processos e procedimentos **(PR.PO-P)**	Gerenciamento de identidade e acesso
Políticas de segurança e privacidade (por exemplo, finalidade, escopo, funções e responsabilidades no ecossistema de processamento de dados e compromisso de gerenciamento), processos e procedimentos são mantidos e usados para gerenciar a proteção de dados. Gerenciamento de identidade, autenticação e controle de acesso **(PR.AC-P)**	Ajuda a integrar a AWS ao ciclo de vida do gerenciamento de identidades e às fontes de autenticação e autorização. Controle de detetive
O acesso a dados e dispositivos é limitado a indivíduos, processos e dispositivos autorizados e é gerenciado de acordo com o risco avaliado de acesso não autorizado. Segurança de dados **(PR.DS-P)**	Fornece orientações para ajudar a identificar possíveis incidentes de segurança em seu ambiente da AWS. Segurança de infraestrutura
Os dados são gerenciados de acordo com a estratégia de risco da organização para proteger a privacidade dos indivíduos e manter a confidencialidade, integridade e disponibilidade dos dados.	Ajuda a implementar metodologias de controle necessárias para cumprir as práticas recomendadas, bem como ajuda a cumprir as obrigações regulatórias ou do setor.
Manutenção (PR.MA-P)	**Proteção de dados**
A manutenção e os reparos do sistema são realizados de forma consistente com políticas, processos e procedimentos.	Ajuda você a implementar salvaguardas apropriadas que protegem os dados em trânsito e em repouso.
Tecnologia de proteção (PR.PT-P)	**Resposta a incidentes**
As soluções de segurança técnica são gerenciadas para garantir a segurança e a resiliência de sistemas, produtos e serviços e dados associados, consistentes com políticas, processos, procedimentos e acordos relacionados.	Ajuda a definir e executar uma resposta a incidentes de segurança.
Categorias NIST Proteger-P (PR-P)	**Recursos de perspectiva de segurança do AWS CAF**

Proteção de dados, políticas, processos e procedimentos (PR.PO-P)	Gerenciamento de identidade e acesso
Políticas de segurança e privacidade (por exemplo, finalidade, escopo, funções e responsabilidades no ecossistema de processamento de dados e compromisso de gerenciamento), processos e procedimentos são mantidos e usados para gerenciar a proteção de dados. Gerenciamento de identidade, autenticação e controle de acesso **(PR.AC-P)**	Ajuda a integrar a AWS ao ciclo de vida do gerenciamento de identidades e às fontes de autenticação e autorização. Controle de detetive
O acesso a dados e dispositivos é limitado a indivíduos, processos e dispositivos autorizados e é gerenciado de acordo com o risco avaliado de acesso não autorizado. Segurança de dados **(PR.DS-P)**	Fornece orientações para ajudar a identificar possíveis incidentes de segurança em seu ambiente da AWS. Segurança de infraestrutura
Os dados são gerenciados de acordo com a estratégia de risco da organização para proteger a privacidade dos indivíduos e manter a confidencialidade, integridade e disponibilidade dos dados.	Ajuda a implementar metodologias de controle necessárias para cumprir as práticas recomendadas, bem como ajuda a cumprir as obrigações regulatórias ou do setor.
Manutenção (PR.MA-P)	**Proteção de dados**
A manutenção e os reparos do sistema são realizados de forma consistente com políticas, processos e procedimentos.	Ajuda você a implementar salvaguardas apropriadas que protegem os dados em trânsito e em repouso.
Tecnologia de proteção (PR.PT-P)	**Resposta a incidentes**
As soluções de segurança técnica são gerenciadas para garantir a segurança e a resiliência de sistemas, produtos e serviços e dados associados, consistentes com políticas, processos, procedimentos e acordos relacionados.	Ajuda a definir e executar uma resposta a incidentes de segurança.
Categorias NIST Controle-P (CT-P)	**Recursos de perspectiva de operações do AWS CAF**
Data processing policies, processes, and procedures (CT.PO-P)	**Monitoramento de serviços**
Políticas, processos e procedimentos são mantidos e usados para gerenciar o processamento de dados (por exemplo, finalidade, escopo, funções e responsabilidades no ecossistema de processamento de dados e compromisso de gerenciamento)	Concentra-se em detectar e responder aos indicadores de integridade das operações de TI, para atender aos seus contratos de nível de serviço e de nível operacional. Monitoramento de desempenho de aplicativos

consistente com a estratégia de risco da organização para proteger a privacidade dos indivíduos. Gerenciamento de processamento de dados **(CT.DM-P)**	Fornece novas abordagens para monitorar o desempenho do aplicativo em um ambiente de nuvem para ajudar você a garantir que a integridade do aplicativo atenda aos requisitos aplicáveis para adoção da nuvem. Gerenciamento de inventário de recursos
	Ajuda a gerenciar ativos virtuais de TI para fornecer serviços de alto desempenho e econômicos.
	Gerenciamento de lançamentos e gerenciamento de mudanças
	Auxilia suas equipes a adotar as melhores práticas de desenvolvimento de software, como automação e técnicas de integração contínua/entrega contínua (IC/EC), aumentando o ritmo de suas inovações.
Os dados são gerenciados de acordo com a estratégia de risco da organização para proteger a privacidade dos indivíduos, aumentar a capacidade de gerenciamento e permitir a implementação de princípios de privacidade (por exemplo, participação individual, qualidade dos dados, minimização de dados) .Processamento desassociado **(CT.DP-P)**	**Relatórios e análises**
	Ajuda a monitorar a integridade dos ativos de nuvem e fornece insights para ajudá-lo a alcançar o nível de desempenho desejado.
	Continuidade de negócios e recuperação de desastres (BC/DR)
As soluções de processamento de dados aumentam a desassociabilidade consistente com a estratégia de risco da organização para proteger a privacidade dos indivíduos e permitir a implementação de princípios de privacidade (por exemplo, minimização de dados).	Ajuda a implementar processos para manter seus negócios funcionando durante um evento catastrófico.
	Catálogo de serviços de TI
	Ajuda você a oferecer serviços em nuvem para a empresa usando um modelo que pode ajudar a melhorar a eficiência do fornecimento de serviços de TI, bem como a produtividade de consumi-los.

Para obter mais detalhes sobre a estrutura do NIST PF, acesse o material público do NIST PF.

Observações finais

Para a AWS, a segurança é sempre nossa principal prioridade. Prestamos serviços a mais de um milhão de clientes ativos, incluindo empresas, instituições educacionais e agências governamentais em mais de 190 países. Nossos clientes incluem prestadores de serviços financeiros e profissionais de saúde, entre outros, e temos a confiança de algumas de suas informações mais confidenciais.

Os serviços da AWS são projetados para oferecer aos clientes flexibilidade sobre como eles configuram e implantam suas soluções, bem como controle sobre seu conteúdo, incluindo onde ele é armazenado, como é armazenado e quem tem acesso a ele. Os clientes da AWS podem criar seus próprios aplicativos seguros e armazenar conteúdo com segurança na AWS.

Para ajudar os clientes a entender melhor como podem atender aos requisitos de privacidade e proteção de dados, incentivamos os clientes a ler os whitepapers de risco, conformidade e segurança, melhores práticas, listas de verificação e orientações publicadas no site da AWS. Esses recursos podem ser encontrados em http://aws.amazon.com/compliance e http://aws.amazon.com/security. Além disso, os clientes podem consultar nosso site de Privacidade de Dados do Brasil disponível em https://aws.amazon.com/compliance/brazil-data-privacy/.

Revisões do documento

Data	Descrição
Março 2022	Primeira publicação