Guia do usuário AWS sobre regulamentações dos serviços financeiros no Brasil – Conselho Monetário Nacional, Resolução 4.658

Julho 2018

aws

[Guia de recursos]

Avisos

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

Sumário

Resumo

Este documento fornece informações que auxiliam as instituições financeiras brasileiras reguladas pelo Banco Central do Brasil, que tem interesse em utilizar ou ampliar o uso dos serviços de nuvem da Amazon Web Services por parte delas.

Introdução

Em 26 de abril de 2018, o Conselho Monetário Nacional (CMN) emitiu a Resolução 4.658 (a resolução do BCB) definindo exigências de segurança cibernética para instituições financeiras brasileiras (IFs) regulamentadas pelo Banco Central do Brasil (BCB), incluindo exigências sobre o uso de serviços de computação em nuvem pelas IFs.

A resolução do BCB define as etapas que as IFs devem seguir para gerenciar riscos de segurança cibernética. Trata-se também da primeira normativa dos reguladores financeiros brasileiros sobre o uso de serviços de nuvem por parte das IFs. A resolução do BCB exige que as IFs avaliem os provedores de nuvem e criem controles internos para gerenciar o relacionamento com o provedor de nuvem. Com isso, a resolução do BCB descreve um caminho para que as IFs possam adotar a nuvem de maneira segura e resiliente. A AWS aprova a clareza dos reguladores financeiros brasileiros e acredita que os clientes da AWS possam utilizar seus serviços de acordo com as expectativas de segurança dos reguladores.

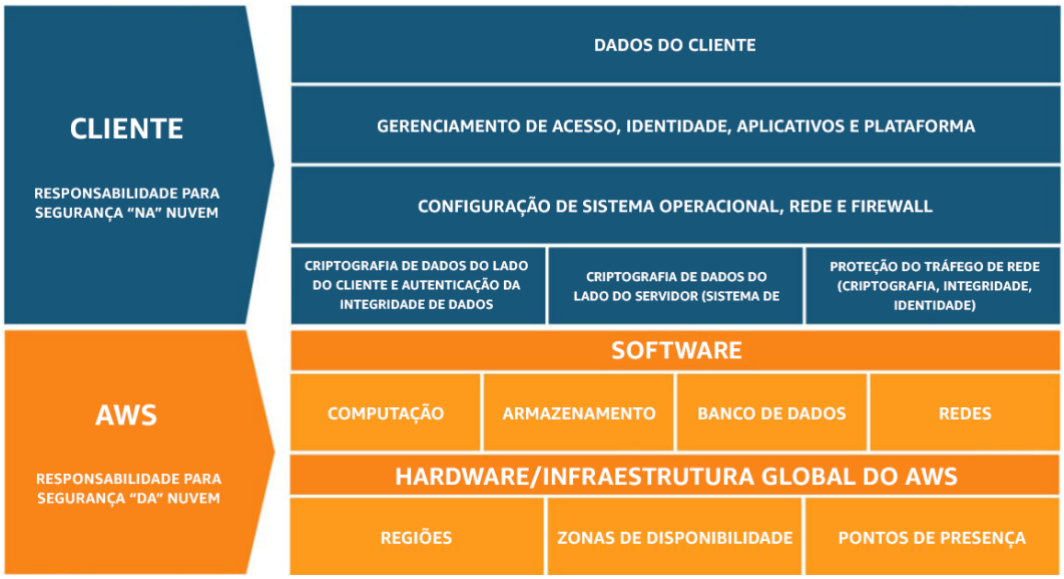
Este guia serve como recurso para ajudar as IFs a compreender os requisitos da resolução do BCB e a desenvolver uma estratégia de adoção de nuvem segura, resiliente e eficiente. As seções a seguir fornecem considerações para as IFs avaliarem suas responsabilidades com relação à resolução 4.658:

- **Segurança e Responsabilidade Compartilhada:** Antes de explorar os requisitos específicos contidos na resolução do BCB, é importante que as IFs compreendam o Modelo de Responsabilidade Compartilhada da AWS. O modelo de responsabilidade compartilhada é fundamental para entender as respectivas funções do cliente e da AWS quanto à segurança. Ele também aborda as etapas que as instituições precisam seguir para garantir conformidade com a resolução do BCB.
- **Programas de garantia de conformidade da AWS:** A resolução do BCB exige, entre outras coisas, que as IFs realizem a devida auditoria dos provedores de nuvem. A AWS conta com certificações e atestados de terceiros referentes a diferentes cargas de trabalho específicas do setor. A AWS também desenvolveu um programa de garantia de segurança (*Security Assurance*) para disponibilizar estes recursos aos clientes. Os clientes podem contar com o programa de garantia de segurança da AWS para auxiliá-los a satisfazer seus requisitos regulatórios.
- **Infraestrutura global da Nuvem AWS:** A infraestrutura global da Nuvem AWS é criada em torno de regiões e zonas de disponibilidade, oferecendo aos clientes uma maneira mais simples e eficaz de desenvolver e operar aplicativos e bancos de dados, proporcionando maior disponibilidade, tolerância a falhas e mais escaláveis do que comparado as infraestruturas de um único datacenter ou mesmo de múltiplos datacenters. Os clientes da AWS podem usar a infraestrutura da nuvem AWS para desenvolver um ambiente consistente com os requisitos de resiliência da resolução do BCB.
- **Resolução do BCB:** Esta seção define as considerações para as IFs utilizarem a AWS; apresentando os requisitos chave para um melhor atendimento às suas necessidades regulatórias.

Tais informações, combinadas, podem ser usadas pelas IFs para iniciar seus processos de auditoria e avaliação sobre como implantar um programa apropriado de segurança da informação, gerenciamento de riscos e governança para o uso dos serviços de nuvem da AWS.

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 regulatórios globais e regionais, além das melhores práticas. No entanto, a segurança na nuvem é de responsabilidade do cliente. Isso significa que são os clientes quem mantem o controle dos programas de segurança que desejam implantar para proteger seu conteúdo, plataforma, aplicações, sistemas e as próprias redes, da mesma maneira que realizam em um datacenter 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 de TI do sistema operacional do host e a camada de virtualização até a segurança física das instalações onde os serviços operam.

Segurança na nuvem

Os clientes são responsáveis pela própria segurança na nuvem. Assim como em um datacenter tradicional, o cliente é responsável por gerenciar o sistema operacional do host (incluindo a instalação de atualizações e patches de segurança) e outros softwares e aplicativos associados, bem como a configuração do firewall do fornecido pela AWS – Security Groups. Os clientes devem escolher cuidadosamente seus serviços, pois suas responsabilidades variam de acordo com os serviços que usam, a integração destes serviços em seus ambientes de TI, além de leis e regulamentações aplicáveis. É importante observar que, ao usar serviços da AWS, os clientes mantêm o controle sobre seu conteúdo e são responsáveis pelo gerenciamento de requisitos críticos de segurança, incluindo:

- O conteúdo que eles escolhem armazenar na AWS.
- Os serviços da AWS que são usados com o conteúdo.
- O país em que seu conteúdo é armazenado.
- O formato e a estrutura deste conteúdo e se ele está mascarado, criptografado ou se é

anônimo.

- Como seus dados são criptografados e onde as chaves são armazenadas.
- Quem tem acesso ao conteúdo e como os direitos de acesso são concedidos, gerenciados e revogados.

Já que são os clientes e não a AWS que controlam estes importantes fatores, são eles que têm responsabilidade por suas escolhas. Os clientes são responsáveis pela segurança do conteúdo que colocam na AWS ou pelo conteúdo que conectam à infraestrutura da AWS, tal como o sistema operacional do host, aplicativos em suas instâncias de computação e conteúdo armazenado e processado por 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 sob diferentes padrões de conformidade e certificações, para poder atender as diversas regiões globais e diferentes tipos de industrias. Os clientes podem usar as certificações de conformidade da AWS para validar a implantação e a eficácia dos controles aplicados pela AWS, incluindo as melhores práticas e certificações de segurança reconhecidas internacionalmente.

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

- **Validação** de que os serviços e instalações da AWS no mundo todo mantêm um ambiente de controle onipresente que opera de maneira eficaz. O ambiente de controle da AWS abrange as pessoas, os processos e a tecnologia necessária para estabelecer e manter um ambiente que dá suporte à eficácia operacional de sua estrutura de controle. A AWS aplica os controles específicos para nuvem identificados pelos principais órgãos do setor de computação em nuvem em seus *frameworks* de controle. A AWS monitora os grupos do setor para identificar as principais práticas que podem ser implementadas e para melhor ajudar os clientes a gerenciar seu ambiente de controle.
- **Demonstração** da postura de conformidade da AWS para ajudar os clientes a verificar a conformidade conforme os requisitos do setor e do governo. A AWS trabalha em conjunto com órgãos externos de certificação e auditores independentes para fornecer aos clientes informações sobre as políticas, processos e controles estabelecidos e operados pela AWS. Os clientes podem usar estas informações para executar seus procedimentos de avaliação e verificação de controles, conforme exigido pelo padrão de conformidade aplicável.
- **Monitorar**, por meio de milhares de requisitos de controle de segurança, assegurando que a AWS mantenha a conformidade com os padrões globais e as melhores práticas.

Programas de garantia de conformidade da AWS

Certificações e atestados de terceiros

A AWS obteve certificações e atestados de auditores terceiros independentes, para diferentes cargas de trabalho específicas do setor financeiro. No entanto, as seguintes são de particular importância para as IFs:

ISO 27001 – é um padrão de gerenciamento de segurança que especifica as melhores práticas de gerenciamento de segurança e controles de segurança abrangentes, conforme as diretrizes de melhores práticas da ISO 27002. A base desta certificação é o desenvolvimento e

implementação de um rigoroso programa de segurança, que inclui o desenvolvimento e a implementação de um sistema de gerenciamento de segurança da informação que delimita como a AWS gerencia a segurança de maneira perpétua, holística e abrangente. Para mais informações ou para fazer download da certificação, consulte a página da web Conformidade ISO 27001.

ISO 27017 – fornece diretrizes sobre os aspectos de segurança da informação da computação em nuvem. Ela recomenda a implantação de controles de segurança da informação específicos da nuvem, que complementam as diretrizes dos padrões ISO 27002 e ISO 27001. Este código de práticas fornece diretrizes adicionais de implantação de controles de segurança de informações, específicas para provedores de serviços em nuvem. Para mais informações ou para fazer download da certificação, consulte a página da web Conformidade ISO 27017.

ISO 27018 – é um código de práticas que aborda a proteção de dados pessoais na nuvem. Ela é baseada no padrão de segurança da informação ISO 27002 e fornece diretrizes sobre a implantação dos controles aplicáveis à PII (Informações de Identificação Pessoal) de nuvens públicas. Ela também fornece um conjunto de controles adicionais e diretrizes associadas destinadas a abordar os requisitos de proteção PII de nuvem pública não abordados pelo conjunto de controles existente da ISO 27002. Para mais informações ou para fazer download da certificação ISO 27018 da AWS, consulte a página da web Conformidade ISO 27018.

ISO 9001 – define uma abordagem focada em processos de documentação e revisão da estrutura, responsabilidades e procedimentos necessários para alcançar um gerenciamento de qualidade eficaz dentro de uma organização. O principal objetivo para a certificação contínua nesse padrão é estabelecer, manter e melhorar a estrutura organizacional, responsabilidades, procedimentos, processos e recursos, de maneira que os produtos e serviços da AWS satisfaçam consistentemente os requisitos de qualidade ISO 9001. Para mais informações ou para fazer download da certificação, consulte a página da web Conformidade ISO 9001.

PCI DSS Nível 1 - O Padrão de Segurança de Dados do Setor de Cartões de Pagamento (Payment Card Industry Data Security Standard), conhecido como PCI DSS, é um padrão de segurança de informações proprietário e administrado pelo Conselho de Padrões de Segurança do PCI. O PCI DSS se aplica a todas as entidades que armazenam, processam ou transmitem dados do portador do cartão (CHD) e/ou dados de autenticação confidenciais (SAD), incluindo comerciantes, processadores, adquirentes, emissores e provedores de serviços. O PCI DSS é exigido pelas bandeiras de cartões e administrado pelo Conselho de Padrões de Segurança do Setor de Cartões de Pagamento. Para mais informações ou para solicitar o Resumo do atestado de conformidade e responsabilidade do PCI DSS, consulte a página da web Conformidade PCI DSS.

SOC – Os relatórios de Controle de Organização e Sistema (SOC) da AWS são relatórios de exame de auditores terceiros independentes que demonstram como a AWS aplica os principais controles e seus objetivos de conformidade. A intenção desses relatórios é ajudar os clientes e seus auditores a entender os controles da AWS que foram definidos para dar suporte às operações e à conformidade. Para mais informações, consulte a página da web Conformidade SOC. Existem três tipos de relatório de SOC da AWS:

- **SOC 1:** Fornece informações sobre o ambiente de controle da AWS que pode ser relevante para os controles internos do cliente sobre relatórios financeiros, além de informações para avaliação e opinião sobre a eficácia dos controles internos sobre relatórios financeiros (ICOFR).
- **SOC 2:** Fornece aos clientes e seus usuários de serviços, conforme sua necessidade de

negócio, uma avaliação independente do ambiente de controle da AWS, relevante para a segurança, a disponibilidade e a confidencialidade do sistema.

- **SOC 3:** Assim como a anterior (SOC 2) fornece os controle da AWS, relevante para a segurança, a disponibilidade e a confidencialidade do sistema, sem divulgar informações internas da AWS.

Ao integrar recursos de serviço que facilitam a auditoria e que têm foco na governança, certificações, atestados e padrões de auditoria, de modo que o modelo de conformidade da AWS permita a aplicação dos programas tradicionais, ajudando os clientes a criar e operar um ambiente na AWS com todos os controle de segurança.

Para mais informações sobre outras certificações e atestados da AWS, consulte a página Programa de garantia da AWS, enquanto para entender sobre a governança e controles de segurança geral e específico dos produto da AWS, consulte o whitepaper Visão geral dos processos de segurança.

AWS Artifact

Os clientes podem usar o AWS Artifact para analisar e fazer download de relatórios e detalhes sobre mais de 2.600 controles de segurança. O AWS Artifact é o portal automatizado de relatórios de conformidade disponível na Console de Gerenciamento da AWS. O portal fornece acesso sob demanda aos documentos de segurança e conformidade da AWS, incluindo os relatórios de SOC, PCI e certificações e acreditações para todas as regiões geográficas e verticais.

Infraestrutura global da AWS

A Infraestrutura da Nuvem AWS é criada em torno de regiões e zonas de disponibilidade. Uma região da AWS é uma localidade física no mundo composta por diferentes zonas de disponibilidade. As zonas de disponibilidade consistem em um ou mais datacenters discretos que estão alojados em instalações separadas, cada uma com energia, rede e conectividade redundante. As zonas de disponibilidade da AWS oferecem aos clientes a capacidade de operar aplicativos de produção e bancos de dados com uma maior disponibilidade, tolerância a falhas e escalabilidade do que seria possível em um único datacenter. A Nuvem AWS opera em 55 zonas de disponibilidade e 18 regiões em todo o mundo. Para obter informações atualizadas sobre regiões e zonas de disponibilidade, consulte a Infraestrutura global da AWS. Os clientes da AWS escolhem as regiões nas quais seu conteúdo e servidores estão localizados. Isso permite aos clientes estabelecer os ambientes que atendem aos requisitos geográficos específicos.

Por exemplo, os clientes da AWS no Brasil podem optar por implantar seus serviços exclusivamente na região da América do Sul (São Paulo) e armazenar seu conteúdo no Brasil, se este for seu local de preferência. Se o cliente fizer esta escolha, o conteúdo será alocado especificamente no Brasil, a menos que o cliente opte por mover tal conteúdo.

A região AWS da América do Sul (São Paulo) foi projetada e construída para atender a rigorosos padrões de conformidade global, proporcionando alto nível de segurança para todos os clientes da AWS. Como em todas as regiões da AWS, a região da América do Sul (São Paulo) está em conformidade com as leis nacionais e globais aplicáveis de proteção de dados.

Resolução 4.658 do BCB

A resolução do BCB exige que as IFs adotem uma política de segurança cibernética que aborde uma ampla variedade de questões de segurança, incluindo o uso de provedores de serviços para processamento de dados, armazenamento físico e computação em nuvem.

Se uma IF deseja usar um provedor de serviços de nuvem, a resolução do BCB exige que ela adote um modelo de governança e políticas de gerenciamento de risco consistentes com a materialidade dos serviços que a instituição está executando em nuvem. A resolução do BCB aponta vários tópicos que a instituição financeira deve levar em consideração ao avaliar um provedor de nuvem, além de especificar determinados termos que devem ser incluídos em um contrato junto ao provedor de serviço de nuvem.

A análise completa da resolução do BCB está além do escopo deste documento. No entanto, as seções a seguir abordam os temas chaves da resolução do BCB e descreve como as IFs podem alavancar o uso dos serviços de nuvem da AWS em conformidade com tais requerimentos.

Implantação da política de segurança cibernética

O Capítulo II, Segmento I da resolução do BCB exige que a IF adote e mantenha uma política de segurança cibernética projetada para garantir a confidencialidade, integridade e disponibilidade de dados e sistemas de informação.

Uma IF pode usar os serviços e a infraestrutura global da AWS para atender aos objetivos de sua política de segurança cibernética. Os serviços da AWS são desenvolvidos para serem seguros por padrão. As IFs também podem utilizar a AWS para alinhamento total com o NIST Cybersecurity Framework (CSF), e assim gerenciar os controles de segurança para os cinco pilares de gerenciamento de riscos (Identificação, Proteção, Detecção, Resposta e Recuperação) alavancando a “segurança na nuvem”.

De acordo com a resolução do BCB, a política de segurança cibernética da IF deve atender a determinados requisitos específicos. Abaixo estão descritos alguns desses requisitos e como a AWS pode ajudar a facilitar seu cumprimento.

Requisito da resolução do BCB	Resposta da AWS
Capítulo II, segmento I, seção 2: A IF implantará e manterá uma política de segurança cibernética baseada em princípios e diretrizes projetados para garantir a confidencialidade, integridade e disponibilidade para os sistemas de dados e informações utilizados.	A infraestrutura da Nuvem AWS foi arquitetada para ser o ambiente de computação em nuvem mais flexível e seguro disponível. A escala da AWS permite um investimento significativamente maior em politicas e contramedidas de segurança do que praticamente qualquer empresa de grande porte poderia pagar sozinha. Essa infraestrutura é composta de hardware, software, rede e as instalações onde os serviços da AWS são executados, fornecendo controles poderosos aos clientes e incluindo controles de configuração de segurança para o tratamento de dados confidenciais, tais como as informações sobre transações financeiras. A AWS ajuda seus clientes a se protegerem contra os ataques cibernéticos, fornecendo diversas ferramentas para proteção de seus dados. Uma lista de recursos e ferramentas está disponível em: https://aws.amazon.com/products/security/. A AWS dá suporte à criptografia TLS/SSL para todos os endpoints da API, além da capacidade de criar túneis VPN para proteger dados em trânsito. A AWS também fornece o AWS Key Management Service (KMS) e dispositivos de hardware dedicados para criptografar dados em repouso, Hardware Security Module (HSM). Os clientes podem optar por proteger seus dados usando os recursos fornecidos pela AWS ou ainda usar suas próprias ferramentas de segurança.
Capítulo II, segmento I, seção 3.II: A política de segurança cibernética da IF deve contemplar, entre outras coisas, os procedimentos e controles internos adotados pela IF para reduzir sua vulnerabilidade a incidentes, além de tratar de outros objetivos de segurança cibernética.	As instituições financeiras podem usar várias ferramentas da AWS para garantir que tenham uma arquitetura mais segura e possam reduzir sua vulnerabilidade a incidentes. Uma ferramenta importante é o Amazon Inspector, um serviço automatizado de avaliação de segurança que ajuda a aprimorar a segurança e a conformidade dos aplicativos implantados na AWS. Ele avalia automaticamente os aplicativos para detectar vulnerabilidades ou desvios das melhores práticas. Depois de fazer a avaliação, o Amazon Inspector gera uma lista detalhada dos problemas de segurança encontrados priorizados por nível de criticidade. Estes problemas podem ser revisados diretamente ou fazer parte de relatórios de avaliação detalhados que estão disponíveis na console ou na API do Amazon Inspector. Os clientes de instituições financeiras também podem usar os serviços da AWS para realizar testes de penetração e testes de

	eventos simulados. Para obter mais informações, visite https://aws.amazon.com/pt/security/penetration-testing/
Capítulo II, segmento I, seção 3.III: A política de segurança cibernética da IF deve contemplar, entre outras coisas, os controles específicos, incluindo aqueles usados para garantir a rastreabilidade dos dados, a fim de proteger informações confidenciais	A AWS oferece aos clientes de instituições financeiras muitas ferramentas para governança e rastreabilidade de dados. O AWS CloudTrail é um serviço que permite governança, conformidade, auditoria operacional e de risco das contas AWS. Com o CloudTrail, os clientes podem registrar, monitorar continuamente e reter a atividade da conta relacionada a ações dentro da infraestrutura da AWS. O CloudTrail fornece o histórico de eventos da atividade da conta, incluindo ações realizadas por meio da Console de Gerenciamento da AWS, SDKs, ferramentas da linha de comando (CLI) e outros serviços da AWS. O histórico de eventos simplifica a análise de segurança, o rastreamento de alterações de recursos e a solução de problemas.
Capítulo II, segmento I, seção 3.V(c) A política de segurança cibernética da IF deve contemplar, entre outras coisas, as diretrizes para a classificação de dados e informações por relevância	A AWS fornece maneiras de categorizar dados organizacionais com base em níveis de confidencialidade. Ao usar tags de recursos, políticas do IAM, AWS KMS e AWS CloudHSM, os clientes podem definir e implantar políticas para classificação de dados.

Implantação de plano de ação e plano de resposta a incidentes

O capítulo II, segmento III da resolução do BCB exige que a IF tenha planos de ação de segurança cibernética e procedimentos de resposta a incidentes estabelecidos.

A AWS implantou uma política e um programa formal e documentado de resposta a incidentes. Estas informações podem ser conferidas no relatório SOC 2 da AWS, disponibilizado aos clientes mediante acordo de não divulgação (NDA). Para obter mais informações, consulte a seção “AWS Artifact”.

Além disso, os clientes podem usar ferramentas como o AWS CloudTrail, Amazon CloudWatch e AWS Config para rastrear, monitorar, analisar e auditar eventos. Se essas ferramentas identificarem um evento analisado e definido como incidente, o "evento de qualificação" gerará um incidente e ativará o processo de gerenciamento de incidentes, além de ações de resposta apropriadas necessárias para a mitigação. Informações sobre como lidar com a resposta a incidentes na nuvem estão disponíveis nesta postagem do blog.

A AWS também mantém boletins de segurança públicos, disponíveis no Centro de Segurança da AWS. Mais detalhes sobre as medidas que a AWS pratica para manter consistentemente os altos níveis de segurança podem ser encontrados no whitepaper Visão geral dos processos de segurança da AWS, disponível em português.

Contratação de serviços de computação em nuvem

O Capítulo III da resolução do BCB exige que as IFs tenham políticas, estratégias e estruturas de gerenciamento de risco em vigor que incluam critérios para o uso de um provedor de serviços em nuvem. A resolução do BCB estabelece critérios específicos que as políticas e procedimentos de gerenciamento de riscos da IF para contemplar o uso de um provedor de serviços em nuvem. A resolução do BCB especifica claramente que as IFs devem adotar práticas de gerenciamento e governança corporativa com relação à terceirização para prestadores de serviços, proporcionalmente à materialidade dos serviços a serem contratados e à exposição da IF a riscos.

A IF pode usar a AWS para atender a todos os requisitos de provedores de serviços em nuvem estabelecidos na resolução do BCB. A tabela abaixo descreve alguns dos requisitos e como a AWS pode ajudar as IFs atendê-los.

Requisito da resolução do BCB	Resposta da AWS
Capítulo III, seção 12.II As políticas e procedimentos de gerenciamento de risco da IF devem contemplar a avaliação da capacidade potencial do provável prestador de serviços para garantir:	
(a) Conformidade com a legislação e regulamentação em vigor	A AWS trabalha em conjunto com órgãos externos de certificação e auditores independentes para fornecer aos clientes informações importantes sobre suas políticas, processos e controles. Os clientes podem usar estas informações para realizar seus procedimentos de avaliação e verificação de controle, conforme exigido pela legislação e regulamentações. Para mais informações sobre as certificações e acreditações da AWS, consulte a página Programa de garantia da AWS.
(b) Acesso da IF aos dados e informações a serem processados ou armazenados pelo provedor de serviços	Os clientes da AWS mantêm a propriedade e o controle dos respectivos dados. A AWS fornece ferramentas simples e avançadas que permitem aos clientes determinar onde seu conteúdo será armazenado, proteger o conteúdo em trânsito e em repouso e gerenciar o acesso a serviços e recursos da AWS para seus grupos e usuários. Os clientes podem fazer um tour virtual pelos datacenters da AWS para entender como são implementados os controles, sistemas automatizados e processos de auditorias terceirizadas para garantir a segurança e a conformidade. Visite https://aws.amazon.com/pt/compliance/data-center/data-centers/
(c) Confidencialidade, integridade, disponibilidade e recuperação de dados e informações processadas ou armazenadas pelo provedor de serviços	A AWS define políticas e procedimentos formais para estabelecer parâmetros comuns aos funcionários sobre os padrões e diretrizes de segurança da informação. A política do sistema de gerenciamento de segurança da informação da AWS estabelece diretrizes para proteger a confidencialidade, integridade e disponibilidade dos sistemas e conteúdo dos clientes. Manter a credibilidade e a confiança do cliente é de extrema importância para a AWS. A AWS realiza um processo contínuo de avaliação de riscos para identificar, avaliar e mitigar riscos em toda a empresa. O processo envolve o desenvolvimento e implantação de planos de tratamento de riscos para mitigá-los conforme necessário. A equipe de gerenciamento de riscos da AWS monitora e escala os riscos continuamente, realizando avaliações em controles recém-

	implantados pelo menos uma vez a cada seis meses. O relatório SOC 2 fornece uma avaliação independente do ambiente de controle da AWS, relevante para a segurança, disponibilidade e confidencialidade do sistema.
(d) Conformidade com as certificações exigidas pela IF para a prestação do serviço contratado	Consulte a resposta ao Capítulo III, Seção 12.I(a), acima.
(e) O acesso da IF a relatórios (elaborados por empresas de auditoria independentes e especializadas, contratadas pelo provedor de serviços) relacionados aos procedimentos e controles utilizados para fornecer os serviços a serem contratados.	A AWS fornece vários relatórios de conformidade de auditores terceirizados que testaram e verificaram a conformidade com base em uma variedade de normas e regulamentos de segurança, incluindo ISO 27001, ISO 27017 e ISO 27018. Para fornecer transparência e eficiência de tais medidas, a AWS dá aos clientes a opção de analisar e fazer download de relatórios e detalhes sobre mais de 2.600 controles de segurança usando o AWS Artifact, que é o portal automatizado de relatórios de conformidade disponível na Console de Gerenciamento da AWS.
(f) Fornecimento de informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados	Os clientes podem ver todas as notificações de segurança por meio do Painel de Status de Serviços da AWS ou do AWS Personal Health Dashboard. Para monitorar anormalidades, os clientes da AWS também podem usar várias ferramentas como AWS CloudTrail, Amazon CloudWatch, AWS Config e AWS Config rules, incluindo as ferramentas disponíveis no Marketplace da AWS.
(g) Identificação e segregação dos dados do cliente da IF usando controles físicos ou lógicos (h) Qualidade dos controles de acesso para proteger os dados e informações do cliente da IF	Mais detalhes sobre as medidas que a AWS implementa para manter consistentemente os altos níveis de segurança podem ser encontrados no whitepaper Visão geral dos processos de segurança da AWS (em português), a Segurança específica do Serviço da AWS pode ser conferida na página 26. O Manual de separação lógica ajuda os clientes a entenderem a separação lógica na nuvem AWS, mostrando suas vantagens em relação a um modelo tradicional de separação física.
Capítulo III, seção 12 § 3 No caso de executar aplicativos pela Internet, a IF deve garantir que o provedor de serviços em potencial adote controles para mitigar os efeitos de quaisquer	Os clientes podem se conectar a um ponto de acesso da AWS via HTTP ou HTTPS usando Secure Sockets Layer (SSL), um protocolo de criptografia projetado para proteger contra espionagem, adulteração e falsificação de mensagens. Para clientes que exigem camadas adicionais de segurança de rede, a AWS oferece o Amazon Virtual Private Cloud (VPC), que

vulnerabilidades quando novas versões do aplicativo forem liberadas.	fornece uma sub-rede privada na Nuvem AWS e a possibilidade de usar um dispositivo de VPN IPsec para criar um túnel criptografado entre a Amazon VPC e seu datacenter.
Capítulo III, seção 12 § 4 A IF terá os recursos e habilidades necessários para a gestão apropriada dos serviços a serem contratados, inclusive para a análise de informações e uso dos recursos previstos no Capítulo III, Seção 12.II(f) (discutido acima)	A IF pode usar os recursos da AWS para garantir que sua equipe tenha o treinamento e os recursos apropriados para gerenciar os serviços da AWS. Os Princípios básicos de segurança da AWS constituem um curso on-line gratuito desenvolvido para apresentar os fundamentos da computação em nuvem e dos conceitos de segurança da AWS, incluindo: Controle de acesso e gerenciamento, governança, registro e métodos de criptografia da AWS. O curso também abrange protocolos de conformidade relacionados a segurança e a estratégias de gerenciamento de riscos, bem como procedimentos relacionados à auditoria de sua infraestrutura de segurança da AWS. Outras opções de treinamento podem ser encontradas em https://aws.amazon.com/pt/training/.
Capítulo III, seção 16 A contratação de serviços de processamento de dados materiais, armazenamento e computação em nuvem fornecidos no exterior deve atender aos seguintes requisitos:	
I. A existência de um acordo para a troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços possam ser prestados;	Para serviços de computação em nuvem prestados no exterior, os clientes devem revisar a lista de MoUs (Memorandos de Entendimento) entre as autoridades dos países e o Banco Central do Brasil, disponível em: http://www.bcb.gov.br/fis/supervisao/memsupervisao.asp?idpai=SUPERVISAOSFN. A lista mostra a existência de acordos para a troca de informações entre o BCB e as autoridades dos países onde os serviços da AWS podem ser prestados.
II. A IF deve assegurar que a prestação dos serviços acima mencionados não cause danos à operação regular da instituição, nem constrangimento à performance do BCB	Os clientes mantêm a propriedade e o controle de seu conteúdo ao usar os serviços da AWS e não cedem essa propriedade ou controle de seu conteúdo à AWS. Os clientes têm controle total sobre quais serviços eles utilizam e quem pode acessar seu conteúdo e seus serviços, incluindo quais credenciais serão necessárias. Os clientes controlam como eles configuram os ambientes e protegem seu conteúdo, inclusive em relação a criptografia do conteúdo (em repouso e em trânsito) e quais outros recursos e ferramentas de segurança eles utilizam e como

	serão utilizados. A AWS não altera as configurações do cliente, estas configurações são determinadas e controladas pelo cliente. Os clientes da AWS têm total liberdade para projetar a arquitetura de segurança a fim de atender às suas necessidades de conformidade. Esta é uma diferença fundamental em comparação com as soluções de hospedagem tradicionais, nas quais o provedor delimita a arquitetura. A AWS permite e capacita o cliente a decidir quando e como as medidas de segurança serão implantadas na nuvem, de acordo com as necessidades de negócios e características de cada cliente.
III. A IF deve definir, antes da contratação, os países e regiões em cada país onde os serviços podem ser prestados e nos quais os dados podem ser armazenados, processados e gerenciados.	Uma lista atualizada de serviços da AWS pode ser encontrada em https://aws.amazon.com/pt/. A Infraestrutura da Nuvem AWS é criada em torno de regiões e zonas de disponibilidade (AZs). As regiões da AWS contam com várias zonas de disponibilidade isoladas e separadas fisicamente, porém conectadas com baixa latência, alta taxa de transferência e redes altamente redundantes. As Zonas de disponibilidade oferecem aos clientes da AWS uma maneira mais fácil e eficaz de desenvolver e operar aplicativos e bancos de dados, tornando-os mais disponíveis, tolerantes a falhas e escaláveis do que as infraestruturas tradicionais de datacenter único ou infraestruturas com múltiplos datacenters. Atualmente, a nuvem AWS abrange 55 zonas de disponibilidade em 18 regiões geográficas e uma região local em todo o mundo. As informações atualizadas estão disponíveis em https://aws.amazon.com/pt/about-aws/global-infrastructure/.
A instituição financeira deve estabelecer alternativas para a continuidade do negócio, em caso de impossibilidade de manutenção ou rescisão do contrato de prestação de serviços	Veja a resposta na seção abaixo: “Plano de continuidade dos negócios”.

Acordos com provedores de serviços em nuvem

O Capítulo III, seção 17 da resolução do BCB exige que as IFs que usam um provedor de serviços de nuvem tenham um acordo contratual que inclua certos termos. Um desses requisitos é que o provedor de serviços em nuvem seja obrigado a notificar a IF sobre a subcontratação de serviços materiais do provedor de serviços em nuvem.

As IFs têm a opção de fazer um Enterprise Agreement com a AWS. Estes acordos dão aos clientes a possibilidade de adaptar seus contratos para melhor atender às suas necessidades, incluindo as

regulatórias. Através de um Enterprise Agreement, a AWS é capaz de oferecer às IFs um contrato que contém os termos relevantes e necessários para atender o Capítulo III, seção 17 da resolução do BCB.

Plano de continuidade de negócios

A resolução do BCB exige que as IFs tenham um plano de continuidade de negócios que inclua determinados elementos. Por exemplo, o capítulo III, seção 16.IV, exige que a IF defina alternativas para o uso de um provedor de serviços em nuvem para continuidade de negócios no caso de impossibilidade de manutenção ou término do contrato de serviços. Além disso, as seções 19 e 20 do capítulo IV exigem que a IF tenha políticas de gerenciamento de riscos que abordem a continuidade de negócios e as respostas a incidentes relevantes.

O Plano de Continuidade de Negócios da AWS detalha o processo que a AWS segue no caso de uma interrupção, desde a detecção até a desativação. Este plano foi desenvolvido para recuperar e reconstituir a AWS usando uma abordagem de três fases: Fase de Ativação e Notificação, fase de Recuperação e fase de Reconstituição. Essa abordagem garante que a AWS realize os procedimentos de recuperação e reconstituição do sistema em uma sequência metódica, maximizando a eficácia dos esforços de recuperação e reconstituição e minimizando o tempo de interrupção do sistema devido a erros e omissões.

A AWS mantém um ambiente de controle de segurança onipresente em todas as regiões. Os clientes usam a AWS para alcançar uma recuperação de desastres mais rápida em seus sistemas de TI críticos, sem incorrer em gastos de infraestrutura de um segundo *site*. A Nuvem AWS oferece suporte a muitas arquiteturas populares de recuperação de desastres (DR), desde ambientes de "pilot light", que estão prontos para serem escalados a qualquer momento, até ambientes de "hot standby", que permitem um failover rápido. Os clientes podem encontrar mais informações sobre como arquitetar um DR na Nuvem AWS aqui: https://aws.amazon.com/pt/disaster-recovery/.

Requisito de notificação

O capítulo III, seção 15 da resolução do BCB exige que as IFs que contratam um provedor de serviços em nuvem notifiquem tal acordo ao BCB pelo menos 60 dias antes da contratação dos serviços. A notificação deve incluir o nome corporativo do provedor de serviços, os serviços relevantes a serem contratados e a indicação dos países e regiões em cada país onde os serviços possam ser fornecidos, e os dados possam ser armazenados, processados e gerenciados.

A AWS considera que a notificação da IF ao BCB é uma ação independente da IF, no entanto, a IF pode aproveitar as informações fornecidas pela AWS para atender às suas necessidades.

Próximas etapas

A jornada de adoção da nuvem em cada organização é única. Para executar com sucesso seu processo de adoção, você precisa entender o status atual de sua organização, o status que a empresa deseja alcançar e a transição necessária para chegar até lá. Saber disso ajudará você a definir metas e criar fluxos de trabalho que permitirão que as equipes tenham sucesso na utilização da nuvem.

O AWS Cloud Adoption Framework (CAF) oferece uma estrutura para ajudar as organizações a desenvolver um plano eficiente de adoção da nuvem. As diretrizes e melhores práticas indicadas na estrutura podem ajudá-lo a criar uma abordagem abrangente para a computação em nuvem em toda a organização, englobando todo o ciclo de vida de TI. O AWS CAF divide o complicado processo de planejamento por áreas de foco gerenciáveis.

Muitas organizações optam por aplicar a metodologia do AWS CAF juntamente com um workshop conduzido por facilitadores, para saber mais sobre estes workshops, entre em contato com seu representante da AWS. Outra alternativa que a AWS fornece é o acesso as ferramentas e recursos de auto atendimento para aplicação da metodologia AWS CAF, visite https://aws.amazon.com/professional-services/CAF/.

Para as IFs no Brasil, os próximos passos normalmente também incluem as seguintes ações:

- Entre em contato com seu representante da AWS para discutir como a rede de parceiros, os arquitetos de soluções, as equipes de serviços profissionais e os instrutores de treinamento da AWS podem ajudar na sua jornada de adoção da nuvem. Caso não tenha um representante da AWS, entre em contato conosco através da página https://aws.amazon.com/pt/contact-us/.
- Obtenha e revise os relatórios mais recentes do SOC 1 e 2 da AWS, o Resumo do atestado de conformidade e responsabilidade do PCI DSS e da certificação ISO 27001. Acesse o portal do AWS Artifact (por meio da Console de Gerenciamento da AWS).
- Avalie a relevância e a aplicação dos whitepapers de segurança da AWS e do Benchmark dos fundamentos da CIS, conforme apropriado para sua jornada de adoção da nuvem e casos de uso. Essas melhores práticas do setor publicadas pelo Center for Internet Security (Centro de Segurança na Internet) vão além das diretrizes de segurança de alto nível já disponíveis, fornecendo aos usuários da AWS recomendações de implantação e avaliação claras e detalhadas.
- Analise mais a fundo práticas de gestão de risco e governança conforme necessário, de acordo com suas exigências de auditoria e avaliação de riscos, usando as ferramentas e os recursos mencionados neste whitepaper e na seção “Leitura adicional” abaixo.
- Fale com seu representante da AWS para obter informações adicionais referente ao Enteprise Agreement.

Leitura adicional

Para obter ajuda adicional, visite os whitepapers de segurança da AWS e confira os seguintes recursos:

- AWS Artifact
- Melhores práticas para resiliência DDoS da AWS
- Lista de verificação de segurança da AWS
- Benchmark dos fundamentos do CIS - AWS
- Web de três camadas CIS da Amazon Web Services
- Proteção de dados em repouso por meio da criptografia
- Melhores práticas para resiliência DDoS da AWS
- Cloud Adoption Framework – Perspectiva de segurança
- Introdução aos Processos de segurança da AWS
- Melhores práticas de segurança da AWS
- Criptografia de dados em repouso
- Risco e conformidade na AWS
- Uso da AWS no contexto de privacidade e considerações de proteção de dados
- Segurança em escala: login na AWS
- Segurança em escala: governança na AWS
- Entrega segura de conteúdo com o CloudFront