À
Comissão de Valores Mobiliários
Rua Sete de Setembro, 111
Centro - Rio de Janeiro
CEP: 20050-901

Ref.: Comentários à Audiência Pública SDM n.º 05/2018 da Comissão de Valores Mobiliários, de 9 de outubro de 2018, referente às alterações na Instrução n.º 505 da Comissão de Valores Mobiliários, de 27 de setembro de 2011, e revogação da Instrução n.º 380 da Comissão de Valores Mobiliários, de 23 de dezembro de 2002.

Vimos pelo presente apresentar os nossos comentários à Audiência Pública SDM n.º 05/2018, de 9 de outubro de 2018, em relação à alteração da Instrução da Comissão de Valores Mobiliários nº 505, de 27 de setembro de 2011 e à revogação da Instrução n.º 380 da Comissão de Valores Mobiliários, de 23 de dezembro de 2002, através da qual a Comissão de Valores Mobiliários ("CVM") apresentou uma proposta para sugestões e comentários.

A Amazon apoia a iniciativa da CVM em promover o diálogo com representantes do setor público e privado para coletar informações e reunir dados para entender a dinâmica do mercado, e a potencial necessidade de alterar uma política e os requisitos para contratar serviços de processamento, armazenamento de dados e serviços de nuvem, a serem observados por corretoras e outras instituições reguladas pela CVM.

A Amazon Web Services, Inc. ("AWS"), uma subsidiária da Amazon.com, Inc., é líder na prestação de serviços de nuvem, com uma vasta experiência mundial na prestação de serviços comerciais em nuvem, para uma base global de clientes. Sendo assim, a AWS adere e cumpre com os mais altos padrões internacionais de segurança, incluindo Certificações e Controles Reconhecidos Internacionalmente para Segurança em Nuvem (conforme resulta do Anexo 1 a este documento).
Devido à nossa experiência na prestação de serviços comerciais em nuvem, contribuimos para as discussões sobre regulamentações de serviços em nuvem por entidades financeiras de diferentes jurisdições em todo o mundo, e gostaríamos de aproveitar esta oportunidade para compartilhar com a CVM algumas das nossas experiências e sugestões sobre o assunto.

Gostaríamos de aproveitar esta ocasião para apontar algumas considerações, sobre as especificidades dos serviços comerciais de nuvem, bem como expressar nossa preocupação sobre o impacto de algumas disposições propostas para o novo regulamento, de forma mais ampla nos mercados de capitais. Há várias oportunidades importantes para fortalecer, em particular, a proposta existente, tal como, adicionar uma definição de serviços em nuvem, e incluir uma

linguagem que reflita como as corretoras e outras instituições financeiras contratam serviços de nuvem.

No entanto, antes de analisar as considerações e práticas recomendadas para as políticas de serviços de nuvem, é importante primeiro definir o que são serviços de nuvem[1] e entender por que eles oferecem um modelo de entrega de TI muito diferente dos métodos tradicionais. Consideramos que a definição e compreensão de serviços de nuvem é crítica, para qualquer discussão e avaliação dos detalhes específicos dessa consulta pública. Serviços de nuvem são a entrega sob demanda de capacidade de computação, armazenamento de banco de dados, aplicativos e outros recursos de TI por meio de uma plataforma de serviços em nuvem baseada na Internet, com preços pagos de acordo com o uso. Independentemente de uma empresa estar utilizando aplicativos que compartilham fotos com milhões de usuários de dispositivos móveis ou apoiando as operações críticas de uma empresa, uma plataforma de serviços de nuvem fornece acesso rápido a recursos flexíveis de TI e de baixo custo.

Os serviços em nuvem fornecem uma maneira simples de acessar servidores, armazenamento, bancos de dados e um amplo conjunto de serviços de aplicativos pela Internet. As plataformas de serviços em nuvem, possuem e mantêm o hardware necessário conectado à rede para esses serviços de aplicativos, enquanto as empresas fornecem e usam o que precisam por meio de um aplicativo da Web. Os serviços de nuvem fornecem aos desenvolvedores e departamentos de TI, a capacidade de se concentrar no que mais importa, evitando o desperdício de tempo e trabalho em funções e tarefas não relacionadas com o do negócio das empresas e com os seus resultados, como a aquisição, manutenção e planejamento da capacidade de infraestrutura de TI.

Como os serviços de nuvem cresceram em popularidade, surgiram vários modelos e estratégias de implantação distintas, para ajudar a atender às necessidades específicas de diferentes usuários. Cada tipo de serviço de nuvem e método de implantação, fornece aos usuários níveis diferentes de controle, flexibilidade e gerenciamento. Existem três modelos principais de serviços de nuvem, são eles: Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e Software como Serviço (SaaS). A IaaS contém os elementos fundamentais básicos para TI em nuvem, e normalmente fornece acesso aos recursos de rede, computadores (virtuais ou em hardware dedicado) e espaço de armazenamento de dados. A IaaS é mais semelhante aos recursos de TI existentes, com os quais muitos departamentos de TI e desenvolvedores estão familiarizados atualmente. O PaaS elimina a necessidade das organizações gerenciarem infraestruturas subjacentes (geralmente hardware e sistemas operacionais) e permite que as entidades se concentrem na implantação e no gerenciamento de seus aplicativos. O SaaS fornece às entidades, aplicativos para o usuário final, que são executados e gerenciados pelo provedor de serviços. Um exemplo comum de um aplicativo SaaS é o e-mail baseado na Web, o qual as organizações podem usar para enviar e receber e-mail, sem precisar gerenciar adições de recursos ao produto de e-mail ou manter os servidores e sistemas operacionais no qual o programa de e-mail está funcionando.

[1] Definição NIST para Computação em Nuvem, SP 800-145, Setembro de 2011 https://csrc.nist.gov/publications/detail/sp/800-145/final

No contexto dos mercados de capitais e seguros, bem como dos bancos de investimento globais, start-ups dos setores tecnológico-financeiro e de pagamentos, os Provedores de Serviços em Nuvem (Cloud Service Providers ou simplesmente "CSPs"), ajudam instituições financeiras a adotar serviços em nuvem para inovar, modernizar e transformar seus ambientes digitais. Serviços em nuvem permitem instituições financeiras oferecer soluções mais inovadoras, reinventar e otimizar seu relacionamento com a tecnologia para reduzir o tempo de lançamentos no mercado, melhorar a experiência de seus clientes e usuários, ser mais eficientes e reduzir custos, bem como automatizar e reforçar a segurança e proteção de dados financeiros e pessoais de seus clientes e usuários. A AWS, como provedora líder de serviços em nuvem, oferece serviços em nuvem em todo o mundo, para todos os tipos de entidades financeiras, independentemente de seu porte ou negócio.

A adesão a serviços em nuvem no setor de serviços financeiros se acelerou nos últimos anos, o que se traduz em maior segurança e flexibilidade para instituições financeiras, em comparação com seus próprios ambientes locais. Os serviços da AWS permitiram que instituições financeiras melhorassem as experiências digitais de seus clientes e usuários, reduzissem seus riscos de crédito e liquidez e se defendessem contra ataques cibernéticos. A AWS elimina barreiras tecnológicas, permitindo que seus clientes financeiros se concentrem no que realmente importa para seus negócios, e inovem e favoreçam novas oportunidades de negócios.

O Banco Capital One[2], por exemplo, um dos maiores bancos dos EUA, oferece cartões de crédito, contas correntes e de poupança, empréstimos para compra de automóveis, recompensas e serviços bancários on-line para consumidores e empresas, e usa a AWS como parte central de sua estratégia de tecnologia. Como resultado, o banco planeja reduzir a quantidade de data center, de oito para três[3] até o final de 2018. Na Austrália, a Suncorp Group[4], uma empresa de serviços financeiros diversificada, administra um ambiente de TI complexo e oneroso para poder suportar 14 marcas e 4 linhas de negócios em 5 países. Reconhecendo que o diferencial da empresa era sua vantagem competitiva, a Suncorp adotou uma cultura de inovação para reimaginar o cenário de TI. Ao escolher a AWS para oferecer suporte a princípios e práticas ágeis, a Suncorp conseguiu lançar uma nuvem virtual privada e um data center virtual em menos de três meses e planeja migrar 2.000 aplicativos para os serviços em nuvem da AWS. Estabelecido em 2000, o Japan Net Bank[5] conseguiu aumentar a confiabilidade e economizar dinheiro, ao hospedar sua plataforma de Administração de Escritório e os recursos de recuperação de desastres, nos serviços em nuvem da AWS. O Japan Net Bank é o único banco na Internet do país, com foco no desenvolvimento e fornecimento de serviços de liquidação para seus clientes. Estes são apenas alguns exemplos públicos que evidenciam o fato de que, os serviços em nuvem, estão possibilitando uma transformação na TI, maior segurança e redução de custos no setor de serviços financeiros em todo o mundo.

[2] https://aws.amazon.com/solutions/case-studies/capital-one/
[3] https://aws.amazon.com/pt/solutions/case-studies/capital-one/
[4] https://aws.amazon.com/solutions/case-studies/suncorp/
[5] https://aws.amazon.com/solutions/case-studies/japan-net-bank/

Assim, em vez de criar regras que possam eventualmente criar obstáculos no uso de serviços em nuvem por empresas de mercado de capitais, acreditamos que a CVM deveria conduzir uma análise profunda para entender como os serviços em nuvem poderiam ajudar o setor de mercado de capitais brasileiro a inovar, desenvolver novos serviços, reduzir despesas de TI e proteger melhor seus sistemas de informação.

Nós acreditamos que é fundamental para a CVM ter uma compreensão profunda dos serviços em nuvem, incluindo especificações técnicas e controles de segurança, como padrões de auditorias terceiras, antes de emitir a nova regra.

Os serviços de nuvem ajudarão não apenas empresas do mercado de capitais a inovar, como dito acima, como permitirão que os reguladores do mercado financeiro utilizem os controles de segurança que os CSPs desenvolveram para inclusive agilizar seu trabalho de supervisão. Por exemplo, ao migrar para a os serviços em nuvem da AWS, a americana FINRA – Autoridade Reguladora da Indústria Financeira[6]— criou uma plataforma flexível que pode se adaptar às dinâmicas do mercado, enquanto fornece aos seus analistas as ferramentas para consultar interativamente conjuntos de dados de inúmeros petabytes. A FINRA é dedicada à proteção do investidor e à integridade do mercado. Ela regula uma parte crítica da indústria de valores mobiliários - empresas de corretagem que fazem negócios com o público nos Estados Unidos. Para responder às rápidas mudanças na dinâmica do mercado, a FINRA transferiu cerca de 90% de seus volumes de dados para a AWS, usando a AWS para capturar, analisar e armazenar um fluxo diário de 37 bilhões de registros.

Ao usar os serviços de nuvem da AWS, os clientes mantêm a capacidade de gerenciar seus próprios requisitos de segurança e conformidade. Como exemplo, a AWS fornece uma ampla variedade de atestados de terceiros, certificações, relatórios de Controles de Organização de Serviços (SOC) e outros relatórios de conformidade relevantes, diretamente para nossos clientes mediante um acordo de confidencialidade[7]. Os relatórios de auditoria e certificações estão disponíveis em um portal[8] de autoatendimento que fornece aos clientes acesso sob demanda à documentação de conformidade que demonstram a conformidade atual, assim como os relatórios de auditoria prévios, da infraestrutura global da AWS, de tal modo que as entidades possam avaliar a conformidade da AWS na linha do tempo. Os clientes podem acessar e baixar todos os artefatos disponíveis a qualquer momento, quantas vezes forem necessárias e sem custo adicional.

Além disso, o ambiente de controle da AWS está sujeito a auditorias regulares internas e externas. A AWS trabalha junto a órgãos externos de certificação e auditores independentes, para analisar e testar o ambiente de controle da AWS. Certificações e atestados internacionais existentes, fornecem um conjunto robusto para cobertura do domínio de segurança para os serviços em nuvem. A Organização Internacional para Padronização (ISO) 27001, o Controle de Organização de Serviço (SOC) e o PCI (Payment Card Industry), da Indústria de pagamento com cartão (“PCI”),

[6] https://aws.amazon.com/solutions/case-studies/finra/

[7] https://docs.aws.amazon.com/pt_br/artifact/latest/ug/what-is-aws-artifact.html

[8] AWS Artifact - Portal de autoatendimento sem custo para acesso sob demanda aos relatórios de conformidade da AWS https://aws.amazon.com/pt/artifact/

em particular, são considerados regimes de garantia de segurança em nuvem, devido à certeza em seus processos e resultados, que foram testados e comprovados como eficazes entre organizações, setores e países que os aplicam:

- ISO 27001 ISO/IEC 27001 é um padrão do Sistema de Gerenciamento de Segurança da Informação (ISMS) publicado pelo ISO e Comissão Internacional Eletrotécnica (IEC). A ISO 27001 é um benchmark de segurança de informações reconhecido internacionalmente, que abrange controles físicos, lógicos, de processos e de gerenciamento. A Associação Brasileira de Normas Técnicas (ABNT) é o órgão responsável pela normalização técnica no Brasil, e usa como referência esta norma como 'ABNT NBR ISO/IEC 27001:2013'.[9]

- SOC 1: O relatório Tipo II de Controles de Organização de Serviço 1 (SOC 1), anteriormente o Relatório de Auditoria de Normas (SAS) Nº 70, relatório de Organização de Serviço (anteriormente chamado de relatório SSAE 16), é um padrão de auditoria amplamente reconhecido, desenvolvido pelo Instituto Americano de Contadores Públicos Certificados (AICPA). O padrão internacional é referido como Normas Internacionais para Compromissos de Garantia No. 3402 (ISAE 3402).

- SOC 2: O relatório de Controles de Organização de Serviço 2 (SOC 2), é um relatório de atestado emitido por uma empresa de Auditoria Contábil Certificada independente (CPA), realizando análises na AT seção 101, Atestado de Comprometimentos[10] (AICPA, Padrões profissionais), para relatar os controles de uma organização de serviços sobre seu sistema, relevantes para segurança, disponibilidade, integridade de processamento, confidencialidade ou privacidade.

Para os controles da AWS, fornecemos informações de controle de TI aos clientes, por meio de um programa de auditoria externa realizada por reconhecidos auditores terceiros. As duas maneiras mais comuns pelas quais os clientes utilizam nosso programa de auditoria são:

1. Definição específica de controle. Os clientes da AWS podem identificar os controles gerenciados pela AWS, por meio de um atestado externo da eficácia operacional, a fim de cumprir os requisitos de conformidade, como a auditoria financeira anual. Para isso, a AWS publica duas vezes por ano, uma ampla gama de controles de TI específicos em nossos relatórios de Controles de Organização de Serviços.[11]

2. Conformidade padrão de controles geral. Se um cliente da AWS exigir que um amplo conjunto de objetivos de controle seja atendido, ele poderá revisar as certificações do setor da AWS, para garantir que os controles auditados estejam alinhados com seus requisitos

[9] ABNT NBR ISO/IEC 27001:2013 https://www.abntcatalogo.com.br/norma.aspx?ID=306580
[10] AICPA: AT 101, Atestado de Comprometimentos https://www.aicpa.org/research/standards/auditattest/downloadabledocuments/at-00101.pdf
[11] Download do relatório SOC 3 da AWS disponível em: https://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf

internos. Com a certificação AWS ISO 27001, a AWS está em conformidade com um amplo e abrangente padrão de segurança e segue as práticas recomendadas para manter um ambiente seguro. A implementação e alinhamento da AWS com a ISO 27001[12] e ISO 27017[13], fornece orientação sobre os aspectos de segurança da informação da computação em nuvem e a ISO 27018[14], é um código de conduta que foca em proteção de dados pessoais de serviços em nuvem. Essas certificações demonstram um compromisso com a segurança da informação em todos os níveis da organização. A AWS é avaliada por um auditor terceirizado independente, para validar o alinhamento com o padrão ISO 27001. A conformidade com esses padrões e códigos de prática reconhecidos internacionalmente, é uma evidência de que o programa de segurança da AWS é abrangente e está de acordo com as melhores práticas do setor. Dada a função dos serviços de computação em nuvem na assistência a instituições financeiras, incluindo as Corretoras de Títulos e Valores Mobiliários (CTVMs) e as Distribuidoras de Títulos e Valores Mobiliários (DTVMs), no fortalecimento de sua postura cibernética, permitindo a inovação e redução de custos. Acreditamos que a Instrução proposta pela CVM, seria aprimorada por mudanças importantes para refletir com mais precisão, os serviços em nuvem e a relação entre entidades de serviços financeiros e CSPs. **Nós escrevemos para pedir que a CVM 1) insira uma definição de serviços em nuvem; 2) insira a aceitação de auditorias de empresas terceiras e certificações internacionais; 3) remova a exigência de acesso físico às instalações quando comprovados por certificações e auditorias externas reconhecidas; 4) esclareça a disposição relativa à subcontratação; e 5) remova ou esclareça a disposição relativa ao acesso a acordos, documentos, dados e informações processados pelo prestador de serviços.**

1. **Para esclarecer o que é computação em nuvem, nós acreditamos que a CVM deveria incluir em suas políticas, a definição de computação em nuvem como sugerido abaixo:**

"*Computação em nuvem, é a entrega sob demanda de capacidade de computação, armazenamento de banco de dados, aplicativos e outros recursos de TI, através de uma plataforma de serviços em nuvem baseada na Internet, com preços pagos conforme o uso*."

2. **Para esclarecer as disposições que dizem respeito à contratação de serviços em nuvem, é essencial que a CVM aceite auditorias e certificações de auditores terceiros reconhecidos, em vez de exigir acesso físico às instalações do data center.**

Os controles de segurança implementados pelos CSPs de Primeiro Nível, como o caso da AWS, desde infraestrutura de data centers, instalações, aos serviços prestados pelos CSPs, somada às certificações internacionais e relatórios de auditoria disponíveis permitem que os reguladores auditem e verifiquem programas de segurança e controles implementados pelos CSPs.

[12] Certificação da AWS ISO 27001 https://d1.awsstatic.com/certifications/iso_27001_global_certification.pdf
[13] Certificação da AWS ISO 27017 https://d1.awsstatic.com/certifications/iso_27017_certification.pdf
[14] Certificação da AWS ISO 27018 https://d1.awsstatic.com/certifications/iso_27018_certification.pdf

A segurança das informações e a validação dos data centers dos CSPs são realizadas por auditores externos independentes e documentados em seus relatórios semestrais, para garantir que o prestador de serviços em nuvem tenha implementado as medidas de segurança adequadas e de acordo com os padrões estabelecidos, para obter certificações de segurança relevantes.

Os CSPs ajudam seus clientes a cumprir seus próprios requisitos de auditoria e regulatórios, além de fornecerem as informações necessárias para que seus clientes possam, por exemplo, executar a análises de riscos e a avaliação dos controles do provedor de serviços em nuvem.

Métodos efetivos de auditoria diferem de acordo com a natureza dos serviços prestados pelo provedor. No caso, os CSPs investem recursos significativos para disponibilizar informações de segurança e auditoria de forma fácil aos usuários dos serviços em nuvem, por meios baseados nos mais altos e reconhecidos padrões da indústria de provedores de serviços em nuvem, incluindo certificações de terceiros, auditorias independentes realizadas por auditores externos e oferecendo ferramentas de auditoria aos acessos lógicos. Esses meios fornecem aos clientes e seus reguladores as informações necessárias para verificar as funções de segurança e auditoria, sem arriscar a segurança física das instalações e infraestrutura dos CSPs.

Os “CSPs de Primeiro Nível” receberam acreditações e certificações reconhecidas internacionalmente em segurança da informação e de sistemas, incluindo controles de segurança física e controles específicos para provedores de serviços em nuvem, como é o caso da certificação ISO 27017, que é o código de boas práticas publicado pela a Organização Internacional de Normalização, ou "ISO", documento traduzido e publicado no Brasil pela ABNT através da referência ‘ABNT NBR ISO/IEC 27017:2016’[15].

A ISO 27001 é um padrão internacional de segurança da informação amplamente reconhecido, que estabelece requisitos e melhores práticas para uma abordagem sistemática para administração da segurança da informação da entidade e baseia-se em uma avaliação de risco periódica apropriada para cenários de ameaças em constante mudança. Para obter tal certificação, uma empresa deve demonstrar que possui uma abordagem sistemática e dinâmica, para o gerenciamento de riscos de segurança da informação que afetam a confidencialidade, integridade e disponibilidade das informações da entidade.

A ISO 27017 é um conjunto de melhores práticas do setor de serviços em nuvem e fornece orientações e recomendações sobre a implementação de controles adicionais de segurança de informação, específicos para provedores de serviços em nuvem, que complementam os padrões da ISO 27001.

A AWS obteve as certificações ISO 27001 e ISO 27017 de seu Sistema de Gerenciamento de Segurança da Informação ("ISMS"), que abrange infraestrutura, data centers e serviços da AWS.

[15] ABNT NBR ISO/IEC 27017:2016 - https://www.abntcatalogo.com.br/norma.aspx?ID=357739

Essa certificação ISMS reforça o compromisso da AWS em fornecer informações relevantes sobre seus controles e práticas de segurança.

Além da implementação de controles de segurança da informação, de acordo com as principais normas internacionais de segurança (como as normas ISO), os CSPs podem receber outras certificações amplamente reconhecidas por instituições financeiras, como o PCI-DSS, Padrão de Segurança de Dados (DSS) da Indústria de Cartões de Pagamento (PCI).

Clientes de “CSPs Primeiro Nível” e reguladores, como a CVM, têm a capacidade de revisar os mecanismos de controle e governança e os principais objetivos de conformidade e segurança implementados pelos CSPs, através dos relatórios de Controles de Organização e Sistema (os “relatórios SOC”).

Os relatórios SOC, são relatórios de auditores externos independentes, que são publicados duas vezes por ano para certificar que os objetivos de controle da entidade auditada são projetados adequadamente e que os controles individuais projetados para proteger os dados de seus clientes, estão funcionando de forma eficaz.

O relatório SOC 2 (Relatório de Segurança, Confidencialidade e Disponibilidade), estende a avaliação dos controles aos critérios estabelecidos pelo Instituto Americano de Contadores Públicos Certificados ("AICPA"), em seus princípios para Serviços de Confiança. Esses princípios definem os principais controles de práticas relevantes para segurança, disponibilidade, integridade de processamento, confidencialidade e privacidade aplicáveis a organizações de serviços, como os CSPs.

No caso da AWS, o relatório SOC 2 avalia o design e eficácia operacional dos controles, que atendem aos critérios de segurança e disponibilidade estabelecidos nos Princípios dos Serviços de Confiança do AICPA. Este relatório fornece transparência adicional à segurança e disponibilidade da AWS com base no padrão de práticas recomendadas do setor, incluindo controles de segurança física, e controles específicos para provedores de serviços em nuvem, e demonstra o compromisso da AWS em proteger os dados de seus clientes.

No caso da AWS, por exemplo, a AWS passa por processos de auditorias realizadas por profissionais externos, que testam a segurança em mais de 2.600 requisitos ao longo do ano. Quando os auditores externos inspecionam os data centers da AWS, eles fazem uma análise detalhada para confirmar se as regras necessárias são seguidas, a fim de obter certificações de segurança internacionalmente relevantes. Dependendo do programa de conformidade e seus requisitos, os auditores externos podem realizar testes para verificar como a mídia de armazenamento é manipulada e descartada, analisar gravações de câmeras de segurança, observar as entradas e corredores de um data center, testar dispositivos de controle de acesso eletrônico e examinar equipamentos de data center.

Existem diferentes meios relevantes disponíveis para que o regulador das instituições financeiras possa exercer plenamente suas funções de supervisão regulatória sobre entidades financeiras, que

usam nuvem de “CSPs de Primeiro Nível”. No caso de auditoria, os relatórios de auditoria e as certificações internacionais são conduzidas por auditores externos independentes, como é o caso do relatório SOC 2 e da certificação ISO 27017, ambos oferecem as informações e os meios necessários para auditar e revisar regularmente os controles, os padrões e as medidas complementares de segurança implementadas pelos CSPs, sem ter que estar fisicamente presente nas instalações ou data centers. De modo a permitir a realização periódica de auditorias de conformidade face aos regulamentos técnicos correspondentes à natureza e ao tipo de atividades terceirizadas.

No caso de uma entidade financeira contratar serviços de TI em nuvem, os “CSPs de Primeiro Nível” fornecem aos seus clientes e entidades que requerem supervisão regulatória, certificações sobre segurança da informações e de sistemas reconhecidas internacionalmente, como a ISO 27017, e relatórios de auditores externos independentes, como os relatórios de Controle de Organização e Sistema, os relatórios do SOC. Para emitir esses relatórios do SOC, o auditor externo audita e analisa os principais controles de práticas relevantes para a segurança, disponibilidade, integridade do processamento, confidencialidade e privacidade, incluindo a segurança física e ambiental dos data centers através dos quais são fornecidos na nuvem, entre outros aspectos.

Em relação às atividades terceirizadas na nuvem, recomendamos que a auditoria seja suficientemente satisfeita, analisando as certificações internacionais de segurança da informação e de sistemas, como a ISO 27017, ou certificações equivalentes, ou ainda, aquelas que as substituam no futuro. Relatórios por auditores externos reconhecidos e independentes, como os relatórios SOC, ou outros relatórios equivalentes, ou ainda, aqueles que os substituam no futuro, que são preparados de acordo com os padrões conhecidos como "SSAE N.º 18" e / ou "ISAE 3402", ou padrões equivalentes, ou ainda, aqueles que os substituem no futuro.

3. Para evitar prejudicar a segurança física, a CVM deve remover o requisito de acesso físico às instalações quando comprovados por certificações e auditorias externas.

Os datacenters dos “CSPs de Primeiro Nível” são seguros por design. De acordo com as melhores práticas internacionais do setor, os CSPs conduzem um processo para avaliar possíveis ameaças para definir a localização das instalações e implementar controles para mitigar os riscos relacionados a sistemas, tecnologia e pessoas. Certificações internacionais e os relatórios de auditoria disponíveis, permitem a CVM auditar e verificar a segurança física da infraestrutura e data centers dos CSPs.

Em termos gerais, os CSPs implementam os seguintes controles físicos e ambientais em seus data centers, entre outros, de acordo com os requisitos aplicáveis das normas internacionais de segurança descritas abaixo:

- Design Seguro: seleção de local, redundância, disponibilidade e planejamento de capacidade.

- Continuidade de Negócios e Recuperação de Desastres: Plano de continuidade de negócios, planos de resposta a situações pandêmicas.
- Acesso físico: Controle de acesso ao data center, regras para empregados e terceirizados.
- Monitoramento e Registro: Revisão, registro e monitoramento de acesso aos datacenters.
- Vigilância e Detecção: Circuito fechado de TV (CFTV), pessoal de vigilancia profissional nos pontos de entrada do data center e sistemas de detecção de intrusão.
- Gerenciamento de Dispositivo: Gerenciamento de recursos, destruição de dispositivos de mídia e armazenamento.
- Sistemas de Suporte à Operação: Energia, condições climáticas e temperatura, detecção e supressão de incêndios, detecção de vazamentos de água.
- Manutenção de Infraestrutura: Manutenção de equipamentos elétricos e mecânicos, gerenciamento do ambiente.
- Governo e Risco: Gerenciamento contínuo dos riscos do data center, acreditação da segurança por auditores terceiros.

No caso de uma instituição financeira contratar serviços em nuvem, o "CSP de Primeiro Nível", indica a o cumprimento de certos padrões internacionais de segurança da informação e de sistemas, (i) as certificações internacionais sobre segurança da informação e de sistemas, como a ISO 27001, ISO 27017 e ISO 27018, ou certificações equivalentes ou ainda, que as substituam no futuro; e (ii) relatórios de auditores externos, como relatórios SOC, ou outros relatórios equivalentes, estão disponíveis para a CVM assim como para a entidade financeira. O auditor da CVM não precisaria acessar fisicamente as instalações de um CSP, para cumprir suas funções de supervisão sobre as atividades terceirizadas em CSP pelas entidades financeiras.

A AWS está extremamente preocupada com as obrigações estabelecidas por essa consulta pública, que exige que os contratos especifiquem onde os CSPs concedem direitos de acesso à CVM para essas instalações. Como discutido acima com respeito a auditorias, este requisito é contrário aos objetivos de segurança e aos princípios de segurança adotados nesta consulta pública. Isso ocorre, pois uma forma importante de os CSPs gerenciarem a segurança de seus data centers limitando o acesso aos detalhes de localização específicos dos datacenters que operam. A obrigatoriedade em divulgar a localização específica dos data centers, prejudicaria as práticas de segurança e tornaria as instalações dos provedores de serviços em nuvem mais vulneráveis.

A supervisão regulatória que obriga a divulgação do endereço de local físico do data center para requisitos de localização de dados, falha em atender aos principais objetivos de sua intenção.

Para esclarecer inicialmente, os clientes de serviços em nuvem da AWS, escolhem a(s) região(ões) na(s) qual(is) o conteúdo será armazenado. Sendo assim, os clientes da AWS conhecem a localização através de uma região (ex. área metropolitana de São Paulo, Brasil). Por motivos de segurança, é fundamental manter a confidencialidade dos endereços físicos de nossas instalações. Para recuperação após desastres e continuidade de negócios onde os clientes optam por armazenar seus dados secundários (backup), não devem confiar nos mesmos componentes de infraestrutura

usados pela localização primária. Como regra muitos provedores de serviços em nuvem adotam uma abordagem geográfica dispersa de toleração a falhas, para garantir que os clientes possam arquitetar seu nível de risco apropriado.

Em resumo, a exigência de acesso às instalações não auxilia no cumprimento do objetivo de metas desejável da CVM. Na verdade, o requisito é contrário aos objetivos de segurança. Sendo assim, incentivamos a CVM a remover esse requisito quando os CSP apresentam comprovações através de certificações e reportes de auditorias externas, a fim de garantir que os clientes possam atingir seus próprios objetivos de segurança, sem comprometer a segurança mais ampla dos serviços em nuvem que eles utilizam.

4. A CVM deve esclarecer sua disposição sobre terceiros subcontratados, referindo-se apenas a terceiros que tenham acesso ou potencial risco de acesso aos dados e conteúdos, inclusive dados pessoais, de propriedade de suas entidades reguladas.

Atualmente, a AWS não usa subcontratantes que tenham acesso, ou potencial risco de acesso, aos dados de propriedade de nossos clientes[16]. A AWS geralmente não terceiriza o desenvolvimento de serviços de computação em nuvem para subcontratados. A AWS mantém acordos formais com seus fornecedores externos e implementa mecanismos apropriados de gerenciamento de seus fornecedores, de acordo com seu relacionamento com a empresa. Os processos de gerenciamento de terceiros da AWS, são revisados por auditores independentes, como parte da conformidade contínua da AWS, por meio dos relatórios SOC (Controles de Organização e Sistema) e das certificações ISO.

Nesse sentido, consideramos que, o que é relevante para as entidades sob vigilância e a CVM, deveria ser se os subcontratados terão acesso aos dados de propriedade das entidades que são processadas na nuvem. Portanto, recomendamos que a CVM esclareça a redação para se referir exclusivamente aos subcontratados, que tenham acesso ou potencial risco de acesso aos dados e conteúdos de propriedade de suas entidades reguladas.

5. A CVM deveria esclarecer ou remover sua disposição sobre o acesso aos contratos, documentos, dados e informações processados pelo provedor de serviços.

A consulta pública exige que a CVM tenha acesso a contratos, documentação, informações, dados e instalações. Com relação aos contratos, documentações e informações, não está claro quais tipos de contratos, documentos e informações estão incluídos nessas categorias. Conforme mencionado anteriormente, os provedores de serviços em nuvem geralmente seguem estruturas de segurança reconhecidas internacionalmente e padrões de certificação (por exemplo, a ISO 27001), que fornecem informações amplas sobre a estrutura de segurança operacional de um provedor de nuvem. Acreditamos que, para o fornecimento de serviços em nuvem e a garantia de segurança, resiliência e integridade de dados, não há necessidade de ter acesso a contratos adicionais, documentação e informações sobre a prestação do serviço. Assim, gostaríamos de solicitar que a

[16] Acesso de subcontratados - https://aws.amazon.com/pt/compliance/third-party-access/

CVM forneça esclarecimentos sobre esta seção, para abordar quais contratos, documentações e informações seriam necessários ou ainda, remover completamente esse requisito.

Mais uma vez, aproveitamos esta oportunidade para parabenizar a CVM por esta iniciativa de debate público sobre um tema de fundamental relevância para o setor e reiteremos a nossa disposição de compartilhar com a CVM a nossa experiência no acompanhamento deste debate em outras jurisdições, bem como em oferecer o que possamos de nosso expertise para esclarecer as questões levantadas acima.

Apêndice 1- Acreditações de segurança em nuvem reconhecidos internacionalmente

No texto abaixo, é apresentada uma visão geral das certificações de segurança da informação e de sistemas amplamente adotadas e reconhecidas internacionalmente, assim como os reportes de auditorias, conduzidos por auditores independentes reconhecidos. A AWS obteve as certificações ou atestados, para cada cada um dos frameworks de segurança relacionados abaixo:

1) ISO 27001, 27002, 27017, 27018

A ISO 27001/27002 é um padrão de segurança amplamente adotado por todo o mundo, que estabelece requisitos e práticas para uma abordagem sistemática, no gerenciamento de informações da empresa e de clientes, com base em avaliações periódicas de riscos adequadas a cenários de ameaças em constante mudança. Para obter a certificação, uma empresa deve demonstrar que possui uma abordagem sistemática e contínua, para gerenciar os riscos de segurança da informação que afetam a confidencialidade, a integridade e a disponibilidade das informações da empresa e dos clientes. Esta certificação reforça o compromisso da AWS, em fornecer informações significativas sobre nossos controles e práticas de segurança. A Associação Brasileira de Normas Técnicas (ABNT) é o órgão responsável pela normalização técnica no Brasil, e usa como referência 'ABNT NBR ISO/IEC 27001:2013'.[17]

A ISO 27017 fornece orientações de implementação em controles de segurança da informação, que se relacionam especificamente aos serviços em nuvem. A AWS obteve a certificação ISO 27017 do Sistema de Gerenciamento de Segurança da Informação (ISMS), abrangendo infraestrutura, data centers e serviços da AWS. A ABNT traduziu e publicou no Brasil através da referência 'ABNT NBR ISO/IEC 27017:2016'[18].

A ISO 27018 é o primeiro código internacional de práticas, que se concentra na proteção de dados pessoais na nuvem. Ela é baseada no padrão de segurança de informações ISO 27002, e fornece orientação para implementação sobre os controles da ISO 27002 aplicáveis às Informações Pessoais Identificáveis (PII) da nuvem pública. Ela também fornece um conjunto de controles adicionais e orientações associadas, destinados a atender aos requisitos de proteção PII de nuvem pública, não abordados pelo conjunto de controles existentes na ISO 27002. A AWS obteve a certificação ISO 27018 para o nosso Sistema de Gerenciamento de Segurança da Informação (ISMS), abrangendo infraestrutura, data centers e serviços da AWS. A ABNT traduziu e publicou no Brasil através da referência 'ABNT NBR ISO/IEC 27018:2018'[19].

2) SOC 1, 2, 3 (Segurança, Confidencialidade, Disponibilidade)

A AWS publica um relatório tipo II de Controles de Organização de Serviço 1 (SOC 1). O relatório SOC 1, audita as certificações para validar que os objetivos de controle da AWS são adequadamente projetados, e que os controles individuais definidos para proteger os dados dos clientes, estão operando de maneira eficaz. O relatório em si, identifica as atividades de controle

[17] ABNT NBR ISO/IEC 27001:2013 https://www.abntcatalogo.com.br/norma.aspx?ID=306580
[18] ABNT NBR ISO/IEC 27017:2016 - https://www.abntcatalogo.com.br/norma.aspx?ID=357739
[19] ABNT NBR ISO/IEC 27018:2018 - https://www.abntcatalogo.com.br/norma.aspx?ID=406634

que respaldam cada um desses objetivos, e os resultados de procedimentos de teste de cada controle são executados por auditores independentes.

Os relatórios SOC 1, estão concentrados nos controles de uma organização prestadora de serviços, que provavelmente serão relevantes para uma auditoria das demonstrações financeiras de uma entidade usuária. Como a base de clientes da AWS é ampla e o uso de serviços da AWS é igualmente amplo, a aplicabilidade dos controles às demonstrações financeiras do cliente, varia de acordo com cada cliente. Portanto, o relatório SOC 1 da AWS é projetado para abranger controles fundamentais específicos, que possam ser necessários durante uma auditoria financeira, bem como abranger uma ampla gama de controles gerais de TI, para acomodar uma ampla gama de cenários de uso e auditoria. Isso permite que clientes aproveitem a infraestrutura da AWS para armazenar e processar dados críticos, incluindo o que é parte integrante de processos de relatório financeiro. A AWS reavalia periodicamente, a seleção desses controles para considerar o feedback do cliente e o uso desse importante relatório de auditoria.

Além do relatório SOC 1, a AWS publica um relatório tipo II de Controles de Organização de Serviço 2 (SOC 2). Semelhante ao SOC 1 na avaliação de controles, o relatório SOC 2 é um relatório certificador, que expande a avaliação dos controles aos critérios estabelecidos pelos Princípios de Serviços de Confiança do Instituto Americano de Contadores Públicos Certificados (AICPA). Esses princípios definem os principais controles de práticas relevantes para segurança, disponibilidade, integridade de processamento, confidencialidade e privacidade, aplicáveis a organizações de serviços, como a AWS. O SOC 2 da AWS, é uma avaliação do design e eficácia operacional dos controles, que atendem as regras dos princípios de segurança e disponibilidade, estabelecidos nos critérios dos Princípios de Serviços de Confiança da AICPA. Este relatório fornece transparência adicional à segurança e disponibilidade da AWS, com base em um padrão predefinido de práticas de mercado, e demonstra ainda mais o compromisso da AWS em proteger os dados do cliente.

A AWS também publica um relatório de Controles de Organização de Serviço 3 (SOC 3). O relatório SOC 3, é um resumo disponível publicamente do relatório SOC 2 da AWS. O relatório inclui a opinião do auditor externo, sobre a operação de controles (com base nos Princípios de Confiança de Segurança da AICPA, incluídos no relatório de SOC 2), além da declaração da administração da AWS sobre a eficácia dos controles e também, uma visão geral da infraestrutura e dos serviços da AWS. O relatório SOC 3 da AWS, inclui todos os data centers da AWS em todo o mundo, que oferecem suporte a serviços do escopo.

3) PCI DSS Nível 1

A AWS está em conformidade com o Nível 1, de acordo com o Padrão de Segurança de Dados (DSS) da Indústria de Cartões de Pagamento (PCI). Os clientes podem executar aplicativos em nossa infraestrutura de tecnologia em conformidade com PCI, para armazenar, processar e transmitir informações de cartão de crédito na nuvem. Em fevereiro de 2013, o Conselho de Padrões de Segurança do PCI, lançou as Diretrizes de Computação em Nuvem do PCI DSS. Essas diretrizes, fornecem aos clientes que gerenciam um ambiente de dados de portadores de cartão, considerações sobre a manutenção dos controles do PCI DSS na nuvem. A AWS incorporou as

Diretrizes de Computação em Nuvem PCI DSS, no Pacote de Conformidade PCI da AWS para os clientes. O Pacote de Conformidade PCI da AWS, inclui o Atestado de Conformidade (AoC) PCI da AWS, que mostra que a AWS foi validada com sucesso, em relação a padrões aplicáveis a um provedor de serviços Primeiro Nível no PCI DSS Versão 3.1 e o Resumo de Responsabilidade PCI da AWS, que explica como a conformidade de responsabilidades, são compartilhadas entre a AWS e nossos clientes na nuvem.

4) CSA

A Cloud Security Alliance (CSA), lançou seu Registro de Segurança, Confiança e Garantia (STAR), um registro gratuito e publicamente acessível, que documenta os controles de segurança fornecidos por várias ofertas de serviços em nuvem, para ajudar os usuários a avaliar a segurança dos CSPs.

A AWS está registrada no CSA STAR e concluiu o Questionário de Iniciativa de Avaliação de Consenso (CAIQ) do Cloud Security Alliance. Este CAIQ publicado pela CSA, fornece uma maneira de referenciar e documentar quais controles de segurança existem, nas ofertas de Infraestrutura como Serviço da AWS.