Orientações para Contratação de Terceiros e Nuvem

SUMÁRIO

INTRODUÇÃO

Nos últimos anos, com a crescente digitalização e busca por processos mais ágeis, flexíveis e escaláveis, a demanda por serviços de computação em nuvem tem crescido entre as instituições dos mercados financeiro e de capitais. A pandemia da covid-19 acelerou essa tendência, uma vez que a implantação do trabalho remoto impulsionou a migração para a nuvem, gerando uma mudança estrutural nos processos de tecnologia e informação das instituições, e a ampliação da dependência dos serviços nas rotinas operacionais. Para além dos potenciais impactos sobre a resiliência operacional das instituições, os reguladores de diversas países têm manifestado preocupações quanto à segurança dos dados pessoais, que são armazenados e computados em nuvem.

Apesar dos esforços regulatórios, a especificidade dos riscos advindos da contratação de serviços de nuvem ainda representa um desafio para as equipes responsáveis pela segurança de informação e cibernética das instituições. A facilidade para contratar soluções de softwares acessados pela internet ampliou significativamente a ocorrência de episódios de Shadow IT nas instituições do mercado de capitais. De acordo com o Nist – National Institute of Standards and Technology, o termo normalmente denota a contratação e o uso de hardware, software ou serviços em nuvem sem o conhecimento da área responsável da instituição, comprometendo sua segurança cibernética. Um exemplo é quando a área de negócios utiliza um programa que não foi aprovado, gerenciado, ou mesmo conhecido pela equipe de tecnologia e informação. Normalmente, as equipes de tecnologia só têm conhecimento quando são acionadas para solucionar incidentes envolvendo o software em questão.

Para mitigar a ocorrência de Shadow IT, é recomendável que as instituições envolvam as equipes de segurança de informação na diligência de terceiros, reduzindo a possibilidade de uma área de unidade de negócios contornar os processos de governança destinados a controlar os riscos de segurança cibernética.

Tendo em vista a estrutura heterogênea do mercado de capitais e a importância da disseminação de conhecimento sobre segurança cibernética, o Grupo Consultivo de Cibersegurança da ANBIMA propôs a elaboração deste documento com melhores práticas para contratação de serviços de informação/tecnologia e nuvem. Este material também tem o propósito educativo de elucidar os riscos e as particularidades da contratação desse tipo de serviço para o público não técnico – principalmente as áreas de Compliance e a alta gestão das instituições. Ela visa, ainda, harmonizar as práticas de cibersegurança da indústria, complementando o Guia de Cibersegurança ANBIMA e facilitando a observância dos requerimentos de segurança da informação e cibernética prescritos nos códigos de autorregulação da Associação.

Esse documento é composto por mais três seções. A primeira apresenta as características gerais da computação em nuvem (modelos de implantação e tipos de serviço) e as considerações de segurança a partir do modelo de responsabilidade compartilhada. Na sequência, detalhamos as recomendações de melhores práticas para contratação de serviços de tecnologia e informação, incluindo nuvem. Por fim, a terceira seção consiste em um **formulário de diligência de segurança da informação/cibernética**, elaborado pelo Grupo Consultivo de Cibersegurança. O documento contém os requisitos mínimos de segurança cibernética que os prestadores de serviços de tecnologia e de informação devem apresentar antes de serem contratados e tem como objetivo apoiar as instituições a estruturarem seus processos de contratação e diligência de terceiros.

COMPUTAÇÃO EM NUVEM

Esta seção apresenta as características gerais da computação em nuvem (modelos de implantação e tipos de serviço) e as considerações de segurança a partir do modelo de responsabilidade compartilhada. **É recomendável que, além da área responsável pela segurança da informação, a de Compliance e a alta gestão das instituições tenham conhecimento dos riscos advindos da contratação dos serviços de nuvem**. Desse modo, este item tem um propósito educativo e traz orientações sobre os aspectos de segurança que devem ser observados no processo de diligência para contratação, avaliação de riscos e monitoramento dos serviços de nuvem.

DEFINIÇÃO E MODELOS DE IMPLANTAÇÃO

Computação em nuvem é um modelo de serviço de TI elástico, escalável que pode ser precificado conforme o uso. Seus principais serviços de computação em nuvem geralmente incluem armazenamento de dados, capacidade de processamento e aplicativos de software. Muitos são semelhantes aos serviços de utilidade pública, pois são amplamente comercializados e podem ser consumidos em pequenas ou grandes quantidades, conforme necessário [1]. De acordo com o Nist, a computação em nuvem possui cinco características essenciais:

- **Autoatendimento sob demanda:** o usuário pode aumentar/reduzir as capacidades computacionais (tempo de servidor, espaço de armazenamento) com base em suas necessidades e de forma automática (sem precisar de interação humana com o provedor de serviços).

1 – Finra (2015)

- **Amplo acesso à rede:** os recursos de nuvem estão disponíveis em uma rede, como a internet pública, que promove o acesso por meio de uma série de clientes, de smartphones a estações de trabalho.

- **Pool de recursos:** o provedor de nuvem agrupa recursos de computação (como armazenamento de dados) que são compartilhados por vários usuários e dinamicamente alocados conforme a demanda do cliente. Os usuários podem ter conhecimento do país em que seus dados estão fisicamente armazenados, mas não sabem a localização exata do data center.

- **Rápida elasticidade:** os recursos de computação podem ser rapidamente ampliados e reduzidos conforme as necessidades dos usuários.

- **Serviços mensuráveis:** todos os serviços são controlados e monitorados automaticamente pela nuvem, de maneira que fica tudo transparente tanto para o consumidor quanto para o fornecedor. Isso ajuda o consumidor a otimizar a utilização da nuvem conforme a produção e o provedor na hora da cobrança dos recursos.

De acordo com o Nist, os modelos de implantação caracterizam amplamente o gerenciamento e a disposição de recursos computacionais para a entrega de serviços aos consumidores, bem como a diferenciação entre as classes desses modelos. Uma **nuvem pública** é aquela em que a infraestrutura e os recursos computacionais que a compõem são disponibilizados ao público em geral pela internet. Ela pertence e é operada por um provedor que fornece serviços de nuvem aos clientes e, por definição, é externo às organizações dos consumidores. O modelo é o mais comum e utilizado pelas instituições, pois, como a infraestrutura mantida pelo provedor é partilhada, ele é mais acessível a vários tamanhos de negócio (menor custo e maior elasticidade).

Na outra extremidade do espectro, estão as **nuvens privadas**. Nelas, a infraestrutura contratada é operada exclusivamente para uma única organização, de modo que a arquitetura de data center e a manutenção dos servidores são planejadas e executadas exclusivamente para uma determinada instituição. A nuvem privada pode ser gerenciada pela própria organização ou por terceiros e pode ser hospedada no data center da organização ou fora dele. Uma nuvem privada tem o potencial de dar à instituição maior controle sobre a infraestrutura, os recursos computacionais e os usuários do que uma pública .

2

2 – Além das nuvens públicas e privadas, existem dois outros modelos de implantação: nuvens comunitárias e híbridas. Para mais, ver Nist (2011).

Embora a escolha do modelo de implantação tenha implicações para a segurança e a privacidade de um sistema, ela não dita o nível de segurança e privacidade da nuvem de forma específica. Isso depende principalmente de garantias, como a solidez das políticas de segurança e privacidade, da robustez dos controles de segurança e privacidade e da transparência dos detalhes de desempenho e gerenciamento do ambiente de nuvem, fornecidos pelo provedor ou alcançado de forma independente pela organização (por exemplo, por meio de testes de vulnerabilidade ou auditoria de operações).

TIPOS DE SERVIÇO

O tipo de serviço de nuvem dita o escopo das responsabilidades do contratante sobre o ambiente computacional, incluindo as considerações de segurança da informação. Usualmente, os serviços são classificados em três tipos:

- **Software-as-a-Service (SaaS)** é um modelo de entrega no qual o consumidor adquire o acesso às aplicações que rodam na infraestrutura de nuvem. Elas podem ser acessadas por vários dispositivos por meio de uma interface (por exemplo, serviço de e-mail e armazenamento acessado pelo navegador ou aplicativo em aparelhos móveis). **Nesse caso, as provisões de segurança são realizadas principalmente pelo provedor de nuvem.** O consumidor não gerencia ou controla a infraestrutura de nuvem subjacente ou aplicações individuais, exceto para seleções de preferência e configurações limitadas.

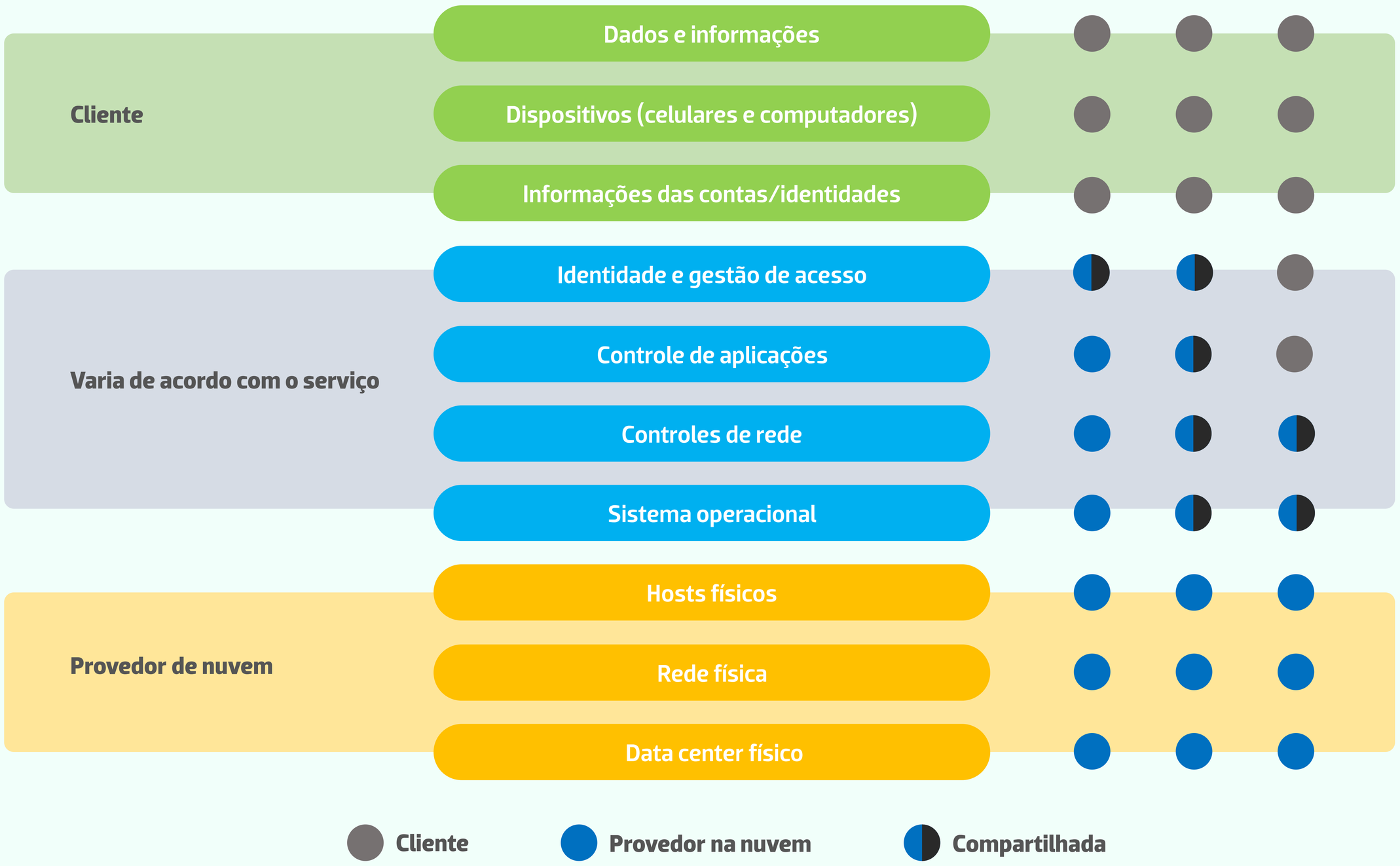
- **Platform-as-a-Service (PaaS)** permite ao consumidor desenvolver ou implantar aplicações na infraestrutura da nuvem e à empresa construir rapidamente soluções personalizadas com a ajuda de ferramentas avançadas. O principal objetivo é reduzir o custo e a complexidade de comprar, hospedar e gerenciar os componentes de hardware e software subjacentes da plataforma de nuvem, incluindo ferramentas de desenvolvimento de banco de dados. O ambiente é determinado pelo provedor e adaptado ao design e à arquitetura da plataforma. O consumidor não gerencia ou controla a infraestrutura (incluindo rede, servidores, sistemas operacionais ou armazenamento), mas tem controle sobre os aplicativos implantados e as definições de configuração do ambiente de hospedagem e da rede. **Nesse modelo, as provisões de segurança são divididas entre provedor e consumidor de nuvem.**

2 – Além das nuvens públicas e privadas, existem dois outros modelos de implantação: nuvens comunitárias e híbridas. Para mais, ver Nist (2011).

Infrastructure-as-a-Service (IaaS) é um modelo que fornece ao consumidor, armazenamento, redes e outros recursos de computação fundamentais, possibilitando a implantação e a execução de softwares, inclusive sistemas operacionais e aplicações. O cliente não gerencia a infraestrutura de nuvem subjacente, mas tem controle sobre sistemas operacionais, armazenamento e aplicações implantadas e sobre os componentes de rede (por exemplo, firewalls de host). **Nesse modelo, o consumidor tem ampla liberdade para escolher o sistema operacional e o ambiente de desenvolvimento, e as provisões de segurança – para além da infraestrutura básica – são realizadas principalmente pelo cliente.**

MODELO DE RESPONSABILIDADE COMPARTILHADA

Compreender o modelo de responsabilidade compartilhada é fundamental para garantir a segurança e a conformidade regulatória. A despeito da maior segurança do ambiente de nuvem – no qual o provedor é responsável pela segurança do ambiente físico e disponibiliza recursos de segurança adicionais –, o cliente ainda fica a cargo de determinados aspectos de segurança que variam em função do tipo de serviço contratado. A definição das responsabilidades das partes é detalhada nos contratos e, no caso de nuvens públicas, geralmente segue o esquema detalhado na figura abaixo:



Apesar de o compartilhamento de responsabilidades entre o provedor de nuvem e o cliente variar conforme o provedor e o serviço contratado (o modelo acima é apenas um exemplo), de modo geral, o consumidor é responsável pela segurança dos dados e das informações armazenados ou processados, incluindo a classificação dos dados (segundo a Lei Geral de Proteção de Dados). A segurança dos dispositivos de acesso, incluindo informações de usuários e das senhas de acesso, também são responsabilidade do cliente. O provedor de serviços de nuvem fica sempre a cargo da segurança da infraestrutura física (data center).

Em relação às responsabilidades que variam de acordo com o serviço contratado e o provedor nuvem, é recomendável dar especial atenção às adicionais de segurança e conformidade nas contratações de serviços de plataforma (PaaS) e infraestrutura (IaaS). Nesses dois casos, é importante que o profissional responsável pela arquitetura dos sistemas em nuvem seja qualificado e realize testes para garantir a segurança da aplicação antes de iniciar o uso.

PRINCIPAIS RISCOS ENVOLVIDOS

Os riscos envolvidos são de difícil mensuração, uma vez que não há informações detalhadas que permitam determinar a probabilidade e o impacto de falhas de segurança com precisão, variando muito pelo tipo de serviço e provedor contratado. Em linhas gerais, os riscos envolvidos concentram-se em:

- **Propriedade dos dados**: é necessário verificar no contrato a existência de cláusula de propriedade, atribuindo-a única e exclusivamente ao cliente e não ao provedor.
- **Acesso aos dados**: trata-se de risco de vazamento ou roubo de dados por acesso indevido. Importante averiguar os mecanismos de controle existentes sobre quem pode acessá-los, contas com privilégios, inclusão e exclusão de acessos, credenciais obsoletas e criptografia.
- **Disponibilidade**: uma vez que os dados estão fora do ambiente do cliente (ou contratante), o controle sobre redundância e a tolerância a falhas será do provedor. Apesar de haver cláusulas que assegurem alta disponibilidade, há o risco de interrupção do serviço. Para avaliação dessa ameaça, deve ser considerado o tempo que a instituição contratante do serviço em nuvem pode ficar com os negócios indisponíveis.

- **Dependência de terceiros:** este é um risco pouco considerado nas avaliações e tem duas vertentes. Primeiramente, o provedor também pode possuir serviços terceirizados, por exemplo, data center ou serviços de segurança, além dos comuns de manutenção, aquisição e instalação de equipamentos. A interrupção na cadeia de fornecimento dos terceiros do provedor traz risco de falhas ou indisponibilidade. Em outra vertente, a migração de provedor, seja ao final do contrato ou a qualquer tempo, não é tarefa simples e corriqueira, acarretando custos adicionais e ajustes nas aplicações. Dada a dificuldade de previsão dos riscos em cadeia, observar os principais pontos de atenção dentro das possibilidades da instituição pode evitar erro ou falhas em sistemas e prejuízos ao negócio.

RECOMENDAÇÕES

As recomendações foram divididas em três partes: diligência pré-contratual; formas de controle; e monitoramento contínuo e encerramento de contrato e acessos.

DILIGÊNCIA PRÉ-CONTRATUAL

O gerenciamento de riscos cibernéticos na contratação de provedor de serviço terceirizado deve ser iniciado antes da assinatura do contrato entre as partes. A primeira prática efetiva que se recomenda é a realização da diligência pré-contratual. Por meio dessa ação, a instituição contratante pode avaliar se as medidas de segurança cibernética do fornecedor em potencial atendem aos padrões da empresa. Como princípio geral, as instituições devem evitar escolher provedores de serviços cujos padrões não estão alinhados com as práticas da principal área de negócios da empresa. Tendo em vista a especificidade dos riscos associados aos serviços de tecnologia e informação, principalmente serviços em nuvem, recomenda-se que:

1. A instituição possua uma estrutura de governança para contratação de terceiros que envolva Compliance, Jurídico,TI, incluindo a área que solicita o serviço. É importante assegurar que as equipes responsáveis pela segurança cibernética/informação realizarão a diligência prévia dos prestadores de serviços de tecnologia e informação para garantir o cumprimento dos requisitos mínimos de segurança cibernética.

- As instituições conscientizem seus funcionários quanto aos riscos cibernéticos advindos da contratação de terceiros, principalmente os de Shadow IT. O ideal é que o tema seja incorporado em treinamentos de segurança cibernética direcionado a todos os colaboradores (incluindo terceiros) das instituições.

- Previamente à contratação de prestadores de serviços de tecnologia e informação, a instituição deve avaliar – com base em riscos – a relevância e a criticidade do trabalho que será contratado e então determinar os controles que serão aplicados. Antes de contratar serviços de processamento e armazenamento de dados e de computação em nuvem (no país ou no exterior), a empresa deve avaliar sua relevância com base na dependência do serviço e na sensibilidade dos dados e das informações a serem processados e, então, determinar os controles que serão aplicados.

- Antes da contratação de serviços de armazenamento, processamento de dados e nuvem, recomenda-se a realização de diligência do prestador de serviços para verificar e garantir que este atende aos requisitos mínimos de segurança e assegure:

  - o cumprimento da legislação e da regulamentação em vigor;
  - o acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;
  - a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;
  - a sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado;
  - o acesso da instituição contratante aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo fornecedor, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;
  - o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

- a identificação e a segregação dos dados dos clientes da instituição por meio de controles físicos ou lógicos;
- a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da instituição.

Recomenda-se, no processo de diligência de prestadores de serviços de nuvem de pequeno e médio porte, solicitar certificados que garantam o cumprimento dos requisitos básicos de segurança e padrões de conformidade regulamentar. Abaixo foram listados alguns exemplos de certificados e relatórios que podem ser pedidos aos prestadores de serviços e que comprovam o cumprimento dos requerimentos mínimos de segurança mencionados no item anterior:

- **SOC 2 tipo II** é o certificado padrão de mercado nos Estados Unidos para atestar a efetividade dos controles de segurança. Relatórios SOC 1 e SOC 3 raramente são exigidos por empresas e órgãos reguladores;
- **ISO/IEC 27001** exigido por muitas empresas e órgãos governamentais na Europa e no Brasil;
- **ISO/IEC 27013** implantação integrada da ISO 27001 e ISO 20000-1 (gestão de serviços de TI);
- **ISO/IEC 27701** extensão da ISO 27001 e 27002, incluindo tópicos relacionados a privacidade;
- **PCI-DSS 3.2.1** exigido para prestadores que armazenam e processam informações de cartão de crédito;
- **SEC 17a-4** necessário para armazenamento em nuvem de dados que não podem ser alterados ou excluídos.

Os grandes prestadores de serviços de nuvem já dispõem de uma série de certificados e relatórios de auditorias realizados por terceiros que comprovam a conformidade com os padrões de segurança requerido pelos reguladores.

FORMAS DE CONTROLE

Termos contratuais adequados

Cláusulas contratuais são uma das formas de controle de riscos, e redigir adequadamente os termos do contrato pode auxiliar a instituição contratante no relacionamento com o prestador selecionado. Recomenda-se que:

- A linguagem seja clara quanto a sensibilidade dos sistemas e das informações aos quais o provedor terá acesso, bem como as obrigações relativas às informações da contratante após o término do relacionamento entre as partes. O rigor das disposições deve ser proporcional ao risco, ou seja, para relacionamentos mais arriscados, recomenda-se linguagem apropriada.

- Sejam elaboradas cláusulas padrão para a contratação de terceiros que assegurem o cumprimento da LGPD (Lei Geral de Proteção de Dados), principalmente na contratação de serviços de armazenamento e processamento em nuvem.

Seguro cibernético

- No processo de diligência de prestadores de serviços, é recomendável checar se o terceiro possui apólice de seguro de responsabilidade e requerer informações sobre a cobertura do seguro contratado – especialmente ao contratar terceiros de pequeno e médio porte. Com base na avaliação de riscos, é possível estimar as perdas financeiras decorrentes da má conduta ou falha na prestação do serviço contratado e averiguar se a cobertura do seguro é suficiente para quitar eventuais prejuízos.

Controles técnicos

- No processo de diligência, a equipe responsável pela segurança cibernética da instituição deve averiguar se o prestador de serviços emprega os controles técnicos adequados para mitigar os riscos de eventuais incidentes cibernéticos (por exemplo, múltiplos fatores de autenticação; single sign on; restrição de acesso a IPs específicos; criptografia de dados em repouso e em trânsito).

MONITORAMENTO CONTÍNUO E ENCERRAMENTO DE CONTRATO E ACESSOS

Após o início da vigência do contrato de prestação de serviços, a contratante deve realizar a diligência contínua do provedor contratado. Essa prática auxilia a empresa na avaliação do cumprimento dos compromissos relativos à segurança cibernética assumidos pelo prestador de serviços no ato da assinatura do contrato. Recomenda-se que:

- A instituição adote o critério baseado em riscos para estabelecer o rigor com o qual será realizada a diligência contínua, ou seja, os fornecedores que têm acesso a dados sensíveis ou sistemas de informação da empresa podem estar sujeitos a um nível mais alto de verificação em comparação com outros provedores.

- Os sistemas e os processos do provedor de serviços terceirizados sejam incluídos no processo geral de avaliação de riscos da instituição contratante. Esse tipo de governança permite identificar vulnerabilidades relativas à segurança cibernética e solicitar tempestivamente a mitigação das vulnerabilidades encontradas no provedor de serviços.

- Até que todos os dados sejam excluídos ou o acesso a eles seja encerrado, o relacionamento com o fornecedor seja incluído no processo de avaliação de risco da empresa e revisado continuamente.

- Juntamente com o fim das relações comerciais entre as partes, os esforços da contratante sejam dedicados à proteção dos dados dos clientes e da empresa aos quais o provedor de serviços teve acesso ou que foram armazenados externamente. Entre os processos mais importantes a serem gerenciados, estão:

  - como a empresa recupera esses dados;
  - como eles são removidos dos sistemas do fornecedor;
  - como essa remoção é documentada;
  - como e quando o acesso do fornecedor aos sistemas da empresa é revogado.

FORMULÁRIO DE DILIGÊNCIA DE SEGURANÇA DA INFORMAÇÃO/CIBERNÉTICA

O documento contém os requisitos mínimos de segurança cibernética que os prestadores de serviços de tecnologia e de informação devem apresentar antes de serem contratados e tem como objetivo apoiar as instituições a estruturarem seus processos de contratação e diligência de terceiros.

Informações gerais

Nome do responsável pela segurança da informação:

E-mail do responsável pela segurança da informação:

Nome do responsável pela proteção de dados:

E-mail do responsável pela proteção de dados:

Tipo de serviço

☐ Nuvem* ☐ Consultoria ☐ Serviços gerenciados ☐ Suporte ☐ Outros

*Se nuvem, assinale:

☐ SaaS ☐ PaaS ☐ IaaS

Descreva o serviço:

1) Quais dados serão processados ou armazenados?

Dados transacionais: informações que rastreiam as interações relacionadas às atividades de uma organização. Normalmente, essas interações são transações comerciais, como pagamentos recebidos de clientes, feitos a fornecedores e movimentação de produtos por meio de estoque, pedidos feitos ou serviços prestados.

De acordo com a LGPD:

Dados pessoais: informação relacionada com pessoa singular identificada ou identificável. Exemplo.: documento de identificação (RG, CPF etc.), endereço, telefone, entre outros.

Dados sensíveis: dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização religiosa, filosófica ou política, dados relativos à saúde ou vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa física.

Selecionar as opções aplicáveis:

Processamento: ☐ transacionais ☐ pessoais ☐ pessoais sensíveis

Armazenamento: ☐ transacionais ☐ pessoais ☐ pessoais sensíveis

Políticas, procedimentos e controles

2) Possui políticas, programa e procedimentos formais relativos à segurança da informação e cibersegurança?

☐ Sim ☐ Não ☐ Em desenvolvimento

Se sim, apresentar cópia do documento.

2.1) O fornecedor possui um contrato explicitando e exigindo requisitos de garantia para confidencialidade, integridade e disponibilidade de dados/informações para outros fornecedores/ parceiros com os quais tenha relações de negócio?

☐ Sim ☐ Não

Se sim, detalhar a cobertura das provisões contratuais.

2.2) As políticas e os procedimentos citados na questão um são testados ou sofrem auditoria periódica?

☐ Sim ☐ Não

Se sim, indicar o período:

☐ meses e apresentar o resultado do último teste e/ou relatório de auditoria

3) Tem plano de resposta a incidente de cibersegurança?

☐ Sim ☐ Não Se sim, apresentar cópia do documento.

4) Possui plano de continuidade de negócios?

☐ Sim ☐ Não Se sim, apresentar cópia do documento.

5) A instituição apresenta ações de conscientização de segurança da informação com seus funcionários?

☐ Sim ☐ Não

Se sim, descrever e informar a frequência.

6) Possui política e/ou procedimento de backup e redundância de informações?

☐ Sim ☐ Não

Se sim, apresentar cópia do documento e informar o tempo estimado para realização do procedimento.

7) Realiza testes periódicos de restore do backup?

☐ Sim ☐ Não

Se sim, informar a periodicidade e apresentar registro do último teste executado.

8) O fornecedor possui um data center alternativo para a recuperação do ambiente tecnológico e de dados, em caso de indisponibilidade do principal?

☐ Sim ☐ Não

Se sim, detalhar as características do data center secundário e o tempo estimado para reinicialização dos serviços.

9) A instituição possui mecanismos de proteção de dados (por exemplo, antispam, firewall, sistema sntivírus, antiphishing, EDR (Endpoint Detection and Response), DLP (Data Loss Prevention), Siem (Security Information and Event Management) e Wapp (Web APP and API Protection)?

☐ Sim ☐ Não

Se sim, descrever.

10) A instituição realiza testes periódicos de verificação de segurança e integridade de sistemas?

☐ Sim ☐ Não

Se sim, indicar periodicidade: ☐ meses.

11) A instituição possui gestão de vulnerabilidades?

☐ Sim ☐ Não

Se sim, descrever.

12) A aplicação possui múltiplos fatores de autenticação (caso a empresa seja uma plataforma de serviços) ?

☐ Sim ☐ Não

Se sim, descrever os métodos de autenticação e os mecanismos de acesso secundário ou recuperação de acesso (no caso de perda do dispositivo/aplicação responsável pelo segundo fator de autenticação).

13) A aplicação possui possibilidade de (SSO) Single Sign-on?

☐ Sim ☐ Não

Se sim, descrever métodos de sincronização para autenticação.

14) A aplicação permite a restrição de acesso a IPs específicos?

☐ Sim ☐ Não

15) A empresa tem processos de criptografia dos dados em repouso e em trânsito?

☐ Sim ☐ Não

Se sim, descrever a tecnologia utilizada.

Segurança e proteção de dados

16) Na prestação de serviços, o contratante irá utilizar armazenamento, processamento e gerenciamento de dados no exterior?

☐ Sim ☐ Não

Se sim, indicar países/localização geográfica.

17) Descrever as ferramentas e/ou os mecanismos utilizados para a proteção dos dados transacionados entre a contratante e a contratada.

18) Descrever as práticas adotadas pela instituição na detecção de atividades não autorizadas e de situações acidentais ou ilícitas de destruição, perda, alteração ou qualquer outra forma nos sistemas utilizados na prestação de serviços. Indicar o responsável, bem como a área e o reporte.

19) Descrever os canais de gestão utilizados em caso de detecção de incidente de cibersegurança, bem como o prazo de registro. Há comunicação a clientes e/ou reguladores?

Outros

20) A instituição possui uma apólice de seguro de responsabilidade?

☐ Sim ☐ Não

Se sim, anexar documento que comprove a contratação da apólice e as informações sobre a cobertura do seguro contratado.

Documentos necessários

- Políticas e procedimentos formais relativos à segurança da informação e segurança cibernética;
- Plano de resposta a incidente de cibersegurança;
- Plano de continuidade de negócios;
- Resultados de testes e auditorias.

ATENÇÃO:

Os documentos solicitados devem ser analisados e aprovados pelas áreas responsáveis pela segurança de informação e cibernética antes da contratação.

REFERÊNCIAS

Finra, 2015. Report on Cybersecurity Practices.

Microsoft, 2017. Shared Responsibility for Cloud Computing.

Nist, 2011. Special Publication 800-145: The NIST Definition of Cloud Computing.

Nist, 2020. Special Publication 800-124: Guidelines for Managing the Security of Mobile Devices in the Enterprise.

RESOLUÇÃO CMN 4.893, 26 de fevereiro 2021.

EXPEDIENTE

Orientações para Contratação de Terceiros e Nuvem

REDAÇÃO
Caroline Miaguti e Andrey Barbato

EDIÇÃO
Ana Flávia Oliveira

PROJETO GRÁFICO
Thiago Dias

PRESIDENTE
Carlos André

VICE-PRESIDENTES
Luiz Sorge, Aroldo Medeiros, Carlos Takahashi, Eric Altafim, José Eduardo Laloni, Pedro Rudge, Roberto Paris e Sergio Cutolo

DIRETORES
Adriano Koelle, Eduardo Azevedo, Fernanda Camargo, Fernando Rabello, Fernando Miranda, Fernando Vallada, Giuliano De Marchi, Gustavo Pires, Julia Wellisch, Rafael Morais, Roberto Paolino, Rodrigo Azevedo e Teodoro Lima

COMITÊ EXECUTIVO
Zeca Doherty, Francisco Vidinha, Guilherme Benaderet, Lina Yajima, Marcelo Billi, Tatiana Itikawa, Amanda Brum, Eliana Marino, Soraya Alves e Thiago Baptista

RIO DE JANEIRO
PRAIA DE BOTAFOGO, 501 – 704, BLOCO II, BOTAFOGO, RIO DE JANEIRO, RJ
CEP: 22250-911
TEL.: (21) 2104-9300

SÃO PAULO
AV. DOUTORA RUTH CARDOSO, 8501, 21º ANDAR, PINHEIROS
SÃO PAULO, SP – CEP: 05425-070
TEL.: (11) 3471 4200

ANBIMA