Cibersegurança | Modelo de Diligência com Terceiros – Incluindo Provedores de Serviços em Nuvem

I. Gestão segura de ambientes terceirizados

Fornecedores, prestadores de serviços e parceiros ("partes externas") podem representar uma fonte significativa de riscos para as instituições em cibersegurança. Nesse sentido a ANBIMA recomenda a verificação da existência de alguns controles, procedimentos e processos junto a esses fornecedores, descritos nas *proposições de questões e documentos* a seguir. Certos cuidados e condutas também são sugeridas nas *recomendações*.

Destaca-se ainda que tais recomendações são aplicáveis àqueles terceiros que a instituição julgue incorrer em riscos de cibersegurança, sobretudo aqueles que gerem acesso a informações e sistemas confidenciais ou sensíveis.

Modelo de diligência com terceiros em cibersegurança – questões

1. Empresa tem políticas, programa e procedimentos formais relativos a segurança da informação e cibersegurança?
    a. Se sim, é objeto de teste ou auditoria periódica?
    b. Se não, está em fase de elaboração? Qual é o prazo de finalização dele para devido envio à instituição contratante?
2. Empresa apresenta plano de resposta a incidentes de cibersegurança?
3. Empresa apresenta ações de conscientização, educação e formação de segurança da informação junto a seus funcionários?
4. Quais são as ferramentas e os mecanismos utilizados para proteção de dados transacionados com a empresa contratante?
5. Quais são as práticas aplicadas para detectar atividade não autorizadas nos sistemas utilizados? Solicitar também designação de responsável por detectar tais atividades e a quem se reporta.
6. Na eventualidade de detecção de incidente de cibersegurança, o relato é feito por meio de canais de gestão apropriadas o mais rápido possível? Há comunicação a clientes e/ou reguladores (quando aplicável)?

Modelo de diligência com terceiros em cibersegurança – documentos a coletar com o fornecedor

- **Programa de segurança cibernética**: se a organização segue políticas, programa e procedimentos formais relativos a segurança da informação e cibersegurança, recomenda-se solicitar envio da documentação à empresa contratante para avaliação e arquivamento. Solicitar também o último relatório de teste/auditoria periódica.
- **Certificações:** solicitar envio de certificações que possam comprovar a devida capacidade técnica do prestador de serviço.

Modelo de diligência com terceiros em cibersegurança – recomendações

- Recomenda-se que as instituições também desenvolvam políticas[1] de verificação dos procedimentos de segurança cibernética de terceiros contratados, avaliando e monitorando periodicamente a capacidade deles de evitar ataques cibernéticos.
- Caso a instituição não apresente políticas, programa e procedimentos formais relativos a segurança da informação e cibersegurança, recomenda-se avaliar o risco de contratar esse prestador.
- Questionar e verificar se a empresa terceirizada contratada apresenta em seu programa ações de gerenciamento de risco com seus fornecedores. Devendo inclusive ser levada em consideração, pela empresa contratante, a possibilidade de alterar ou impedir a subcontratação ou terceirização de serviços para outros prestadores.
- Estabelecer o nível de diligência de acordo com o risco que a relação com o fornecedor pode criar para a instituição.
- Dar atenção especial a fornecedores que recebem e/ou tratam dados considerados confidenciais ou de clientes, bem como para aqueles que têm conexões lógicas (links) com a instituição. O que envolve, conforme necessário, discussão e verificações de políticas e procedimentos dos fornecedores a respeito de cibersegurança, além de possíveis visitas às instalações e até mesmo verificação de eventuais subcontratações.
- Definir os papéis e as responsabilidades de colaboradores junto aos fornecedores, definidas e documentadas de acordo com a política de segurança da informação da organização.
- Estabelecer canal seguro e formal para troca de informações entre o prestador e a instituição, especialmente prevendo comunicação de incidentes.
- É recomendável a formalização da aprovação desses terceiros nos organismos internos responsáveis, com revisão de tais aprovações periodicamente.
- Elaborar contratos de prestação de serviço que contemplem cláusulas de confidencialidade e/ou contratos de NDA (Non Disclosure Agreement) e demais disposições específicas relacionadas ao risco cibernético nos contratos de serviços.
- Ao se identificar deficiências nas respostas e no envio de documentação, recomenda-se propor ações de remediação para atingir tais objetivos.

[1] Alguns códigos de regulação e melhores práticas da ANBIMA exigem, em determinadas situações, que a instituição mantenha política interna que descreva seus processos de seleção, contratação e monitoramento de prestadores de determinados serviços.

II. Segurança básica na utilização de infraestrutura na nuvem

De acordo com o NIST (National Institute of Standards and Technology)[2], a computação em nuvem é definida como um modelo que permitir acesso, de modo conveniente e sob demanda, a um conjunto de recursos computacionais configuráveis e compartilhado (por exemplo, redes, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente provisionados e liberados com o mínimo de esforço de gerenciamento ou interação com o provedor de serviços. A evolução na disponibilidade e sofisticação de tais serviços permitiu novos recursos para empresas e usuários, trazendo benefícios como redução dos custos, maior flexibilidade e escalabilidade, velocidade e balanceamento de carga.

Também de acordo com o NIST, este modelo de nuvem promove maior disponibilidade e é composto por cinco características essenciais: autoatendimento sob demanda; acesso amplo à rede; agrupamento de recursos; rápida elasticidade; e serviço mensurado. Destacam-se ainda três modelos de serviços[3]: (i) Software as a Service (SaaS) – utilização do software do provedor por meio de subscrição, eliminando a necessidade de instalação e execução nos computadores; (ii) Platform as a Service (PaaS) – desenvolvimento, teste, uso e controle sobre softwares próprios; e (iii) Infrastructure as a Service (IaaS) – utilização e controles sobre softwares próprios e de terceiros, sistemas operacionais, servidores, unidades de armazenamento e rede – contratação de servidores virtuais.

Nesse sentido, a computação em nuvem pode ser considerada como uma forma de contratação de serviço de terceiros e, assim como as demais contratações de fornecedores externos, envolve determinados riscos que devem ser levados em conta pela instituição, demandando certos cuidados proporcionais a esta identificação de ameaças. Requerendo especial atenção em alguns controles internos, segurança de sistemas e privacidade das informações.

Abordagem também seguida pelo FFIEC (Federal Financial Institutions Examination Council)[4], órgão federal norte-americano voltado à promoção de uniformidade na supervisão de instituições financeiras. Este chama a atenção para questões como necessidade de diligência com o provedor de serviço; gestão de fornecedor, sobretudo com foco na proteção de dados de usuários e informações sensíveis; auditoria; e identificação de riscos regulatórios e reputacionais.

[2] Ver NIST *Cloud Computing Program* – NCCP, disponível em (acesso em 13/9/17): https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp.

[3] Ver também *Regulação Sobre Serviços Terceirizados de Computação em Nuvem* (Ricardo Freitas Valle Vaghi, maio de 2017).

[4] Ver *Outsourced Cloud Computing* (FFIEC, 10/7/12). Disponível em (acesso em 13/9/17): https://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf