Guia Sindusfarma de Qualificação de Fornecedores para Serviços na Nuvem

31

Jair Calixto

SINDUSFARMA

Guia Sindusfarma de Qualificação de Fornecedores para Serviços na Nuvem

Jair Calixto
(Coordenação)

Volume 31 2019

Mensagem da Diretoria

A Diretoria do Sindusfarma tem o prazer de levar aos profissionais das empresas associadas e a todos os interessados no setor farmacêutico o "Guia Sindusfarma de Qualificação de Fornecedores para Serviços na Nuvem".

Os avanços da tecnologia de informação têm exigido a formação de profissionais cada vez mais capacitados em gerir e garantir a segurança dos conteúdos disponíveis em sistemas informatizados internos e externos (nuvem).

A presente publicação tem o objetivo de orientar os profissionais das empresas do Complexo Produtivo da Saúde sobre as melhores práticas de gestão nesse novo campo, reafirmando o permanente compromisso da entidade com a qualificação e atualização constantes dos profissionais do setor.

Nelson A. Mussolini
Presidente Executivo

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro)

Guia Sindusfarma de qualificação de fornecedores para serviços na nuvem [livro eletrônico] / [coordenação] Jair Calixto.
-- São Paulo : Sindusfarma, 2019.

900 Kb ; PDF

Vários colaboradores.

Bibliografia.

1. Computação em nuvem 2. Computação em nuvem - Medidas de segurança 3. Indústria farmacêutica 4. Informação - Sistemas de armazenagem e recuperação 5. Infraestrutura de tecnologia da informação 6. Serviços da Web I. Calixto, Jair.

19-31021 CDD-004.6782

Índices para catálogo sistemático:
Cloud computing : Serviços : Ciência da computação 004.6782
Cibele Maria Dias - Bibliotecária - CRB-8/9427

Número de ISBN
978-85-60162-73-4

Apresentação

Com o passar dos anos, grande parte dos dados dos sistemas computadorizados estão em servidores externos (nuvem).

A utilização da computação em nuvem é bem aceita em vários setores, inclusive nas indústrias das chamadas "Ciências da Vida", mas requer a adoção de uma série de avaliações prévias e precauções, com a finalidade de ajustá-la às necessidades de cada segmento econômico e mitigar eventuais problemas.

Nesse sentido, esperamos que este Guia contribua para orientar os profissionais do setor sobre os melhores processos de contratação e manutenção desses bancos de dados, com pleno conhecimento dos benefícios e riscos que as novas tecnologias digitais oferecem.

Jair Calixto
Diretor de Assuntos Técnicos e Inovação

Colaboraram com a construção deste material

- Ana Padovini
- Andre Goto
- Diego Kise
- Giselle Gataz
- Heloisa Kronemberger
- Neilton Leite
- Rafael Almeida
- Silvia Martins

Coordenação

- Jair Calixto
- Silvia Martins

Quer fazer parte deste time?

Contribua para o aprimoramento deste Manual compartilhando suas impressões e sugestões através do e-mail **qualidade@sindusfarma.org.br**.

Sumário

Introdução

1. Introdução

Com o passar dos anos os sistemas computadorizados, sejam eles embarcados nos equipamentos ou nas ferramentas de gestão, passaram a gerar muitas informações manuais e apenas uma pequena parte desses dados passaram a ser armazenados em servidores locais. Para gerenciá-los, diversos profissionais foram e estão sendo capacitados para compor as equipes de tecnologia da informação das empresas de ciências da vida.

Com o aumento da necessidade de armazenamento de dados, os custos cresceram exponencialmente e surgiu um segmento de mercado de tecnologia da informação no qual empresas especializadas no fornecimento de espaço virtual se responsabilizam em fornecer a infraestrutura e serviços agregados para garantir a disponibilidade dos dados dos contratantes desses serviços.

Esse tipo de serviço foi bem-aceito em diversos ramos da economia, principalmente naqueles que precisavam responder ao mercado de forma rápida, sem perder seu 'core business,' como por exemplo, os bancos.

Devido aos investimentos feitos pelo sistema bancário, com o objetivo de deixar seus fornecedores mais eficientes e seguros, as empresas do segmento de ciências da vida, que assistiram seus fornecedores bancários a adotarem o uso de serviços na nuvem, passaram a questionar como essa tecnologia poderia ajudá-los a evoluir, melhorando seus processos e reduzindo custos.

Entretanto, o principal questionamento refere-se como podemos garantir que tais tecnologias, apesar de reduzir os custos operacionais no armazenamento de dados, não se tornem uma vulnerabilidade importante.

Dessa maneira, por iniciativa do SINDUSFARMA, foi criado um grupo de colaboração voluntária dos associados para desenvolver este guia com os principais riscos e ações mitigatórias recomendadas.

Esperamos que com a leitura deste guia, as indústrias de Ciências da Vida possam se orientar de como contratar e manter a parte de suas informações em banco de dados externos ("na nuvem"), tendo pleno conhecimento dos riscos e dos benefícios decorrentes da adoção de tais tecnologias.

Nota: *este Guia foi escrito com base nas literaturas e normas relacionadas a seguir, baseadas na interpretação e experiência dos autores. Podem não refletir exatamente os termos e textos originais devido à liberdade de tradução para melhor entendimento do leitor e para a realidade das empresas de Ciências da Vida, foco deste Guia*.

Objetivo do Guia

2. Objetivos

Suportar os processos de qualificação e validação dos fornecedores de serviços em nuvem.

Definições e Conceitos

3. Definições e Conceitos

API: Interface de Programação de Aplicações. Deve-se assegurar a métrica de logs e alarmes para acessos indevidos às aplicações e interfaces. Esse monitoramento auxilia na averiguação de erros das aplicações e a reduzir o tempo de detecção de atividades mal-intencionadas.

Balanceamento de carga: Técnica para distribuir a carga de trabalho uniformemente entre dois ou mais computadores, enlaces de rede, discos rígidos ou outros recursos, a fim de otimizar a utilização de recursos, maximizar o desempenho, minimizar o tempo de resposta e evitar sobrecarga.

Backup: Dado copiado a fim de proteção em caso de perda de integridade ou disponibilidade do dado original.

Contratada: Qualquer pessoa física ou jurídica devidamente identificada no documento de acordo com o nível de serviço, doravante denominada contratada.

Ciências da Vida: Compreende às empresas dos segmentos farmacêutico, farmoquímico, produtos médicos, higiene pessoal, perfumes, cosméticos, alimentos, gases medicinais, saneantes, veterinária, distribuição e armazenamento e respectivos fornecedores.

Contratante: Responsável pela contratação de um serviço, cliente.

Hypervisor: É um software, hardware ou firmware que roda ou cria as máquinas virtuais. Ele controla os acessos dos sistemas operacionais visitantes aos dispositivos de hardware.

Incidente: Interrupção não planejada em um serviço de TI ou redução na qualidade desse serviço. Qualquer evento que pode afetar um serviço de TI no futuro, também é um incidente.

NDA: Non Disclosure Agreement (Acordo de Confidencialidade).

Restore: Retornar uma configuração ou serviço de TI a um estado de funcionamento. Isso se inicia com a recuperação de um serviço de TI, incluindo a recuperação de dados a um estado consistente, conhecido. Após a recuperação é decidido se outras etapas são necessárias antes que o serviço de TI possa ser disponibilizado para os outros usuários.

SLA: Um acordo de nível de serviço (ANS) ou service level agreement (SLA) é um documento formal, acordado por ambas as partes (contratante e contratada), que definem um conjunto de objetivos de níveis de serviços. Esses objetivos podem abordar a disponibilidade, desempenho, segurança, conformidade e privacidade.

'Transparência ou transparente para o usuário final': termo utilizado para expressar que uma funcionalidade ou automatismo é imperceptível para o usuário que está operando uma plataforma, ou seja, o usuário não consegue perceber o que está ocorrendo 'por trás' da funcionalidade

Glossário

4. Glossário

3PAOs	Third Party Assessment Organizations.
BPx	Boas Práticas x (Fabricação, Laboratório etc.).
BSA	Business Software Alliance.
CSA	Cloud Security Alliance.
CVE	Common Vulnerabilities and Exposures.
FedRAMP	Federal Risk and Authorization Management Program.
FIPS	Federal Information Processing Standard.
FISMA	Federal Information Security Management Act.
GDPR	Regulamento Geral sobre Proteção de Dados.
HD	Hard Disk (Disco Rígido).
HIPAA	Health Insurance Portability in Accountability Act (Lei de Responsabilidade e Portabilidade de Provedores de Saúde).
IaaS	Infrastructure as a Service (Infraestrutura como serviço).
IEC	International Electrotechnical Commission.
IMDA	Info-communications Media Development Authority.
IP	Internet Protocol.
ISO	International Organization for Standardization.
LAN	Local Area Networks (Rede Local).
MFA	Multi Factor Authentication (Autenticação de Múltiplo Fator).
MTCS	Multi-Tier Cloud Security.
NIST	National Institute of Standards and Technology.
PaaS	Plataform as a Service (Plataforma como serviço).
PII	Personally Identifiable Information (Informação pessoalmente identificável).
SaaS	Software as a Service (Software como serviço).
SOC	Security Operation Center (Centro de Operações de Segurança).

SS	Singapore Standard.
SSD	Solid-State Drive.
SSL	Secure Socket Layer.
TI	Tecnologia da Informação.
TLS	Transport Layer Security.
UK – NCSC	United Kingdom’s National Cyber Security Centre.

O que é Nuvem

5. O que é Nuvem

Muitos podem não perceber, mas a Computação em Nuvem já faz parte da rotina da maioria das pessoas. Uma prova disso são os aplicativos que carregamos no smartphone, e que fornecem desde informações do trânsito até a quantidade de medicamento que se deve tomar. Essas aplicações funcionam e armazenam os dados em um servidor online, para que possam ser acessados pelas pessoas de qualquer lugar. A alusão ao termo "nuvem" se faz justamente por essa característica da aplicação e os dados ficarem armazenados em um ambiente online, acessível a qualquer momento, através de usuários autenticados, independente de sua localização física.

Conforme cresce a confiança das empresas em relação à computação em nuvem, para serviços e aplicativos, cresce também o grau de preocupação com relação à segurança e seu adequado funcionamento quando comparado com o armazenamento local na empresa.

Nuvem (Cloud) é uma forma de entregar aplicativos e recursos de TI. É a capacidade de armazenamento e cálculo de computadores, e servidores compartilhados e interligados por meio da internet, que fornece acesso aos serviços de infraestrutura ou para fornecedores que desejam disponibilizar os seus aplicativos aos usuários.

Os aplicativos essenciais ao negócio ficam até hoje em sua maioria armazenados em uma sala da TI (Tecnologia da Informação), ou datacenter, na sede da empresa, o que é chamado 'on-premises'. Mas o que é servidor on-premises? É o uso de servidor e recursos de TI dentro da empresa sob sua responsabilidade, ou seja, a companhia utiliza a sua infraestrutura interna em vez de serviço remoto para processar suas aplicações de hardware e software.

Na opção on-premises, a empresa tem de ter disponibilidade de espaço físico para operação dos equipamentos, com instalações seguras contra incidentes, como incêndios, chuvas, desabamentos, furtos, roubos, estrutura de piso elevado para passagem de cabos, sistema de ar condicionado para evitar aquecimento nos servidores etc. Esse modelo exige alto investimento inicial na compra de hardware e software. Muitas empresas ainda mantêm essa estrutura on-premise, mas outras encontram-se em fase de transição, migrando para o uso desses serviços em nuvem.

Porém, quando pensamos nesses serviços ligados à nuvem, ou seja, de infraestrutura e de software, esses passam a ser adquiridos de fornecedor externo especializado. Assim, o fornecimento do serviço em nuvem se divide em três categorias, são elas:

a) SaaS – software como serviço – o fornecedor é responsável por toda estrutura que será usada, e o cliente tem acesso à aplicação de software final (incluindo a infraestrutura para armazenamento do software e dos dados gerados pela aplicação, mediante o pagamento de uma mensalidade ou anuidade;

b) PaaS – Plataforma como serviço – a equipe de infraestrutura é responsável apenas pelas aplicações, e o fornecedor é responsável por toda a estrutura para manter essa aplicação disponibilizada aos usuários;

c) IaaS – Infraestrutura como serviço – a infraestrutura fica a cargo do fornecedor, e o contratante fica responsável pela administração do espaço e servidores adquiridos.

5.1. Nuvem pública, privada ou híbrida? Entenda as diferenças

a) Nuvem Pública — a nuvem pública é o modelo mais utilizado nas empresas, por ser adequada à utilização de softwares, como serviços (SaaS) e permitir a ampliação da capacidade de armazenamento. Assim, os serviços são fornecidos em um ambiente virtualizado, acessível por meio da internet, construído utilizando recursos físicos agrupados e compartilhados;

b) Nuvem Privada — a nuvem privada foi criada para atender às necessidades de um único negócio. Ela pode ser implementada internamente para atender a diversas filiais, por exemplo, ou ser fornecida por um provedor. É uma arquitetura de data center própria e exclusiva de uma empresa;

c) Nuvem Híbrida — a nuvem híbrida mescla os dois modelos anteriores, visando a extrair o melhor de ambos e desempenhar funções distintas dentro de uma mesma organização. Se por um lado as nuvens públicas oferecem mais escalabilidade do que as privadas, essas, por sua vez, são as mais recomendadas para armazenagem de dados críticos.

Quando nos deparamos com a menção de nuvem, na maioria das vezes, os profissionais estão se referindo à internet pública. Entretanto, vários tipos de rede podem ser chamados de nuvem.

Há nuvens públicas baseadas na internet pública, há nuvens privadas baseadas em internet privada e nuvens híbridas que são uma combinação das duas. Em razão da quantidade de versões de nuvem, nem todas as empresas ficam satisfeitas com o mesmo tipo de solução. É possível que a empresa esteja utilizando um tipo de aplicativo, como e-mail, que funciona bem mesmo com o desempenho variável da nuvem pública. Porém, certos usuários, como por exemplo, órgãos do governo, instituições financeiras e provedores de saúde, apresentam preocupações com relação à privacidade e segurança oferecidas pela internet pública.

Se estiver planejando utilizar a nuvem pública, será necessário um provedor de serviços de internet que ofereça alto desempenho e confiabilidade. Quando a nuvem pública não é segura o bastante, ou quando o desempenho é de crucial importância, as instituições do governo e outros tipos de negócio podem se sentir mais à vontade com nuvem privada.

Dependendo dos requisitos da empresa, um único tipo de nuvem pode não ser suficiente para atendê-la, sendo necessária a utilização de diferentes tipos de nuvem. Assim, é comum que fornecedores de serviços de infraestrutura tenham plataformas que facilitem tal migração dos dados de um tipo de nuvem para outro.

À medida que as empresas migram suas funções essenciais para a nuvem, a escolha do provedor torna-se essencial, pois, quanto maior a capacidade do provedor de nuvem em entregar seus aplicativos e recursos, melhor será a ex-

periência do usuário. Dessa forma, para eficaz escolha do produto a ser adquirido, é necessário listar os prós e contras do tipo de serviço (privada, pública ou híbrida), levando em consideração a criticidade da aplicação, armazenamento de dados sigilosos, e também considerar o custo. Após a escolha do tipo de serviço, é necessário partir para a escolha do provedor.

Com diferentes sistemas sendo utilizados em uma mesma empresa, pode ser necessária a utilização de serviços de webservice. Essa é uma solução utilizada para a integração de sistemas e a comunicação entre diferentes aplicações. Com essa tecnologia é possível que aplicações possam interagir com aquelas que já existem, e que sistemas desenvolvidos em plataformas diferentes, sejam compatíveis. Um exemplo desse tipo de serviço são os operadores logísticos ou força de vendas, que necessitam processar arquivos oriundos de empresas e/ou aplicações diferentes. Então, esses provedores de webservices processam os arquivos de fora, verificando um conjunto de regras, liberando tais arquivos para serem processados pelo ERP (Enterprise Resource Planning) da empresa, por exemplo. Se os arquivos que tais empresas processam dados, que impactam na qualidade do produto, saúde do paciente ou consumidor ou ainda na integridade e/ou privacidade de dados, esse fornecedor também deve passar pelo processo de qualificação e é objetivo deste Guia.

Este Guia tem o objetivo de contemplar itens que devem ser considerados para qualificação do serviço ou aplicação para empresas reguladas da área de Ciências da Vida ou, ainda, colaborar na escolha do serviço correto. É importante, nessa fase, que a equipe de TI trabalhe em conjunto com a equipe de Garantia da Qualidade.

Soluções de Nuvem para todas as Empresas de Ciências da Vida

6. Soluções de Nuvem para todas as Empresas de Ciências da Vida

Os fornecedores de serviço em nuvem possuem uma base diversa de clientes – desde usuários individuais, que simplesmente querem salvar alguns arquivos, até empresas multinacionais em uma ampla gama de indústrias. A representação e importância do mercado farmacêutico para os fornecedores de serviço em nuvem não é tão grande quanto os outros; e essa presença limitada, resulta em poder limitado para ditar como o processo de negócio na nuvem deve operar em aspectos de qualidade.

Um exemplo dessa limitação é o fato de que alguns dos grandes fornecedores de serviço em nuvem (e um dos mais economicamente viáveis) possam estar relutantes em abrir suas empresas e processos para um exame minucioso de uma equipe de auditores multidisciplinar, já que podem ter um atestado de atendimento a requerimentos GxP (por exemplo, GXP. [2018]. Disponível em: <https://aws.amazon.com/pt/compliance/gxp-part-11-annex-11/>. Acesso em: 07 nov. 2018., Considerations for Using AWS Products in GxP Systems. [2018]. Disponível em: <https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_GxP_Systems.pdf>. Acesso em: 07 nov. 2018.).

Os fornecedores que abrem suas portas para auditorias nem sempre entendem à necessidade de auditorias individuais das empresas regulamentadas e preferem que seja fornecido por elas um "Certificado BPx". Entretanto, esse certificado não existe! Nesse caso, uma opção é o atestado de atendimento a requerimentos BPx, conforme exemplo anterior.

Além de grandes provedores de serviços de nuvem, há aqueles menores, os quais são capazes de criar uma configuração sob demanda para atendimento aos requerimentos BPx de cada empresa, porém por serem serviços mais personalizados, o custo é consideravelmente maior, tornando-os pouco atraentes no aspecto econômico. Devido a isso, a opção pelos grandes provedores de serviço em nuvem, que já possuem uma configuração para atendimento aos requerimentos de mercado, além dos requerimentos BPx, torna-se mais atraente de um ponto de vista econômico e de conformidade regulatória.

Há uma ampla gama de indústrias que já usam esses serviços, incluindo as indústrias mais "conservadoras", como o setor bancário. Então, por que os processos são suficientes para o setor bancário e não são bons o suficiente para grandes empresas reguladas? Certificações especializadas para empresas são possíveis (CMMI, ISO etc.). As certificações vão desde controles gerais de um provedor até certificações específicas da área, como segurança.

Nesse caso, como as empresas farmacêuticas então devem proceder?

É importante que a Garantia da Qualidade, junto ao setor de TI, e os fornecedores sejam parceiros para entender os requerimentos da entrega dos serviços de nuvem antes de realizar julgamentos quanto à qualidade do processo e avaliar "por que", "onde" e "por quem" os controles são estabelecidos, e então verificar "que" controles são esses.

Para entender e melhor gerenciar os riscos – e não simplesmente evitá-los – que acompanham a tecnologia em nuvem, deve-se criar uma estrutura para gerenciar tais riscos, tanto internos quanto referentes aos processos de gerenciamento de fornecedores. Para tal, existe e é referência no mercado, a Cloud Security Alliance (CSA), que é uma organização mundial dedicada à definição e conscientização das melhores práticas para ajudar a garantir um ambiente seguro de computação em nuvem. A CSA aproveita a experiência no assunto de profissionais do setor, associações, governos e seus membros corporativos e individuais para oferecer pesquisa, educação, certificação, eventos e produtos específicos para a segurança da nuvem. As atividades, o conhecimento gerado e ampla rede da CSA beneficiam toda a comunidade impactada pela nuvem - provedores, clientes, governos, empreendedores e a indústria - e fornece um fórum por meio do qual diversas partes podem trabalhar juntas para criar e manter um ecossistema de nuvem confiável.

A CSA é focada em fornecer maneiras aceitas pelas empresas de Ciências da Vida de documentar quais controles de segurança existem nos serviços de IaaS, PaaS e SaaS, fornecendo transparência no controle de segurança.

Uma das ferramentas para avaliar o provedor de nuvem é o Questionário de Iniciativa de Avaliações de Consenso (Consensus Assessments Initiative Questionnaire – CAIQ (Disponível em: https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v3-0-1/ Acesso em: 07 de maio de 2019), que fornece maneiras aceitas pelo setor farmacêutico de documentar quais controles de segurança existem nas ofertas de IaaS, PaaS e SaaS. O questionário (CAIQ) está disponível no formato de planilha e fornece um conjunto de mais de 140 perguntas que um consumidor de nuvem e um auditor em nuvem podem solicitar a um provedor. Os provedores podem optar por enviar um Questionário de Iniciativa de Avaliação de Consenso preenchido pelo próprio fornecedor. Para mais detalhes, veja item 8.2 deste documento.

6.1. Sobre a Autoavaliação da CSA STAR

O CSA STAR Self Assessment é aberto a todos os provedores de nuvem, e permite que eles enviem relatórios de autoavaliação que documentam a conformidade com as práticas recomendadas publicadas pela CSA.

Desde o lançamento inicial do programa de autoavaliação, no final de 2011, a CSA teve um impacto positivo na adesão dos provedores de grande porte e outros menores, visto que esses reconheceram a necessidade de fornecer maior transparência e garantia dos seus serviços, diante da solicitação, por parte dos usuários finais e corporações, a respeito da visibilidade dos controles de segurança fornecidos por esses provedores de computação em nuvem.

Os provedores de nuvem podem enviar dois tipos diferentes de relatórios para indicar sua conformidade com as práticas recomendadas da CSA: CCM (Cloud Controls Matrix) e Formulário de autoavaliação.

A Cloud Controls Matrix (CCM) fornece uma estrutura de controles detalhada dos conceitos e princípios de segurança ao provedor, alinhados à orientação da Cloud Security Alliance, em 13 domínios (temas). Como uma estrutura, a CSA

CCM fornece às organizações a estrutura, os detalhes e a clareza necessários relacionados à segurança da informação sob medida para o setor de nuvem. Os provedores podem optar por enviar um relatório documentando a conformidade com a Cloud Controls Matrix.

A autoinspeção para publicação é uma prática encorajada pela CSA para todos os fornecedores de IaaS, SaaS e PaaS, grandes e pequenos. Com o preenchimento da autoavaliação, os provedores abordarão algumas das perguntas de segurança mais urgentes e importantes que os compradores estão fazendo e podem acelerar drasticamente o processo de qualificação e compra de seus serviços.

A outra ferramenta é o questionário CAIQ, o qual já foi descrito anteriormente.

6.2. Sobre a Certificação CSA STAR

A certificação CSA STAR é uma avaliação rigorosa independente de terceiros sobre a segurança de um provedor de serviços em nuvem. A certificação de tecnologia aproveita os requerimentos do padrão de gerenciamento de sistema ISO / IEC 27001 junto com o CSA Cloud Controls Matrix, um conjunto específico de critérios que medem os níveis de capacidade do serviço em nuvem.

As organizações que terceirizam serviços para provedores de nuvem têm várias preocupações sobre a segurança de seus dados e informações. Ao obter a Certificação STAR, os provedores de nuvem de todos os tamanhos serão capazes de fornecer aos clientes em potencial uma maior compreensão de seus níveis de controles de segurança.

A certificação STAR baseia-se em atender a norma ISO/IEC 27001 e no conjunto de critérios especificados na CCM. A avaliação independente por um organismo de certificação acreditado da CSA atribuirá uma pontuação de "capacidade de gestão" a cada um dos domínios de segurança da CCM. Cada domínio será pontuado em uma maturidade específica e será medido em relação a alguns princípios de gerenciamento.

O relatório interno mostrará às organizações quão maduros são os processos dos provedores de serviço de nuvem, e quais áreas eles precisam considerar a melhoria para atingir um nível ideal de maturidade. Esses níveis serão designados como "Não", "Bronze", "Prata" ou "Ouro". Organizações certificadas serão listadas no Registro CSA STAR como "STAR Certified" (Star Certification. [2019]. Disponível em: <https://cloudsecurityalliance.org/star/certification/#_overview>. Acesso em: 15 mar. 2019.).

A certificação CSA STAR permite que o auditor (cliente) avalie o desempenho de uma empresa em termos de sustentabilidade e riscos a longo prazo, além de garantir que eles sejam conduzidos pelo SLA, permitindo que a alta administração da contratante quantifique e meça a melhoria ano após ano.

Arquiteturas de Aplicações em Nuvem

7. Arquiteturas de Aplicações em Nuvem

7.1. Modelos de Aplicações em Nuvem

Existem basicamente alguns modelos de aplicações em nuvem que dependem de como funciona a estrutura do sistema SaaS, os mais comuns:

1) Fornecedor que publica as mudanças para todos os clientes de uma única vez, não tendo como diferenciar um cliente do outro;
2) Fornecedor que publica as mudanças que são iguais para todos os usuários, porém em tempos diferentes para cada cliente;
3) Fornecedor que trata configuração/código distinto para cada cliente.

É importante que seja verificado no momento da contratação se o fornecedor de nuvem segue as práticas de controle de versão seguindo o procedimento escrito, aprovado e funcionários treinados.

O conceito inicial de nuvem é que a infraestrutura ou software não estejam hospedados fisicamente nas instalações da empresa. Existem aplicações SaaS que são disponibilizadas na mesma versão para todos os clientes e usuários no mesmo momento. Também existem aplicações SaaS que são disponibilizadas em novas versões para os clientes em momentos diferentes. O desafio é o processo de gerenciamento das novas versões, muitas vezes conduzidas e determinadas pelo fornecedor, que pode não ter o conhecimento para o devido estudo do impacto das mudanças no processo em andamento e tempo de validar/qualificar as novas funcionalidades.

Sabemos que as empresas da área de Ciências da Vida não podem aceitar nova versão do sistema diretamente em ambiente de produção, por ferir as boas práticas BPx.

Veja um exemplo:

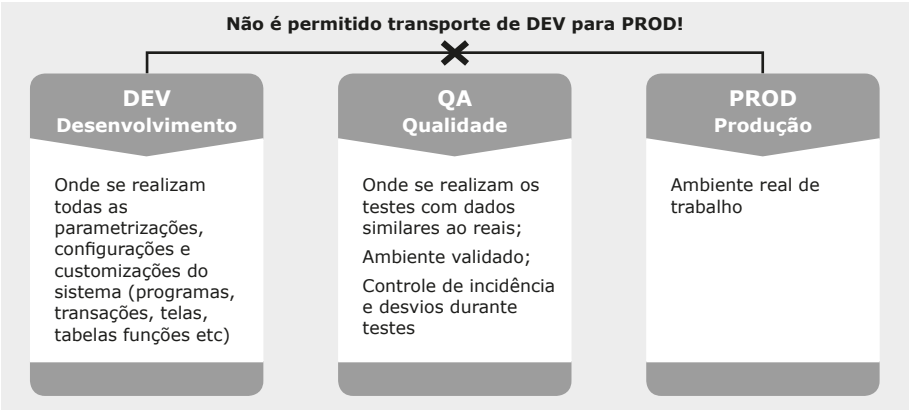

Figura 1 - Transporte de Versões entre Ambientes

Em algumas empresas, o ambiente de QA (Quality Assurance) ilustrado na figura anterior também pode ser chamado de outros nomes, por exemplo: ambiente de homologação, ambiente de testes etc.

No momento da contratação do vendor do sistema SaaS, é importante garantir que o fornecedor tenha a boa prática de emitir Release Notes como um documento formal indicando claramente quais são as mudanças, em linguagem clara, que permita aos usuários idenficar corretamente as alterações da próxima versão. Eventualmente, o nome desse documento pode sofrer mudanças de acordo com a estratégia de cada fornecedor, porém é importante garantir que o vendor não disponibilizará nova versão do sistema sem que deixe claro com adequada antecedência quais mudanças pretende disponibilizar.

O Release Notes é ferramenta para que a equipe multidisciplinar do cliente faça análise BPx relevante das mudanças.

É importante garantir que os fornecedores disponibilizem o ambiente intermediário entre o desenvolvimento e o ambiente de produção e que seja adotada por ambos (cliente e fornecedor) a boa prática de validar as novas funcionalidades.

O fornecedor de SaaS focado em indústrias de Ciências da Vida normalmente adota a boa prática de elaborar o Release Notes e disponibiliza-o aos seus clientes com antecedência acordada em contrato em conjunto com a disponibilização dessa nova versão em ambiente de qualidade para que a equipe do cliente possa providenciar os testes formalizados das mudanças antes da entrada das novas funcionalidades em ambiente de produção.

Recomenda-se garantir que o fornecedor preveja horas para participar da Análise de Riscos Funcional em conjunto com o cliente e/ou que o fornecedor disponibilize informações detalhadas à respeito das novas funcionalidades como Manual do Usuário e telas indicando exatamente tais mudanças e respectivos impactos nas funcionalidades existentes. O Release Notes é importante para guiar tal trabalho, contudo, geralmente não contempla informações detalhadas necessárias para a condução da Análise de Riscos Funcional, como o próprio nome diz, analisar como as mudanças irão operar para, assim, definir o grau do risco e, se necessário, mitigá-lo. A estratégia de testes é definida nessa fase.

Recomenda-se que pelo menos as seguintes etapas críticas devam ser previstas antes da nova versão do sistema ser disponibilizada:

1) Receber o Release Notes do fornecedor listando as mudanças em linguagem clara para os usuários com antecedência suficiente;
2) Análise BPx relevante pela equipe multidisciplinar do usuário (impacto ou não ao produto, ao paciente ou consumidor e à integridade de dados);
3) Análise de Riscos Funcional das funcionalidades classificadas como BPx relevantes;
4) Definir medidas de controle para os riscos médios e altos;
5) Definir estratégia de testes, cenários de testes e critérios de aceitação;
6) Executar os testes em ambientes de qualidade;

7) Utilizar as funcionalidades da nova versão que tenham sido aprovadas e todas as ações de medida de controle comprovadamente implementadas.

Observação: podem ocorrer casos em que nem todos os testes sejam aprovados, assim como pode ocorrer situações do cliente não ter controle sobre a disponibilização da nova versão na nuvem em ambiente de produção. Nesse caso, ações de contingência ou cobertas por procedimentos podem ser utilizadas com decisões baseadas em riscos.

7.2. Esteira DevOps

O termo DevOps deriva da junção das palavras "desenvolvimento" e "operações", sendo uma prática de engenharia de software que possui o intuito de unificar o desenvolvimento e a operação de software.

O termo 'esteira DevOps' é utilizado para referir-se às entregas contínuas, metodologias ágeis que sistematizam e organizam os fluxos de trabalho que ajudam a produzir esteira de entregas integrando as áreas de desenvolvimento e áreas ligadas à operação do sistema.

Existem algumas soluções de software no mercado que propõe o uso automático do sistema para publicação da aplicação em ambiente de produção, porém, nesse caso, esse sistema necessita de validação prévia com estratégia baseada em riscos.

7.3. Conceito de Tenant

O modelo SaaS requer tecnologias e arquiteturas especificamente desenhadas para operar em nuvem. O que acontece é que as aplicações Multi-Tenant, pela forma como são estruturadas, permitem a adição de novos locatários ou inquilinos (tenants) com certa facilidade, o que se encaixa na forma de utilização do SaaS.

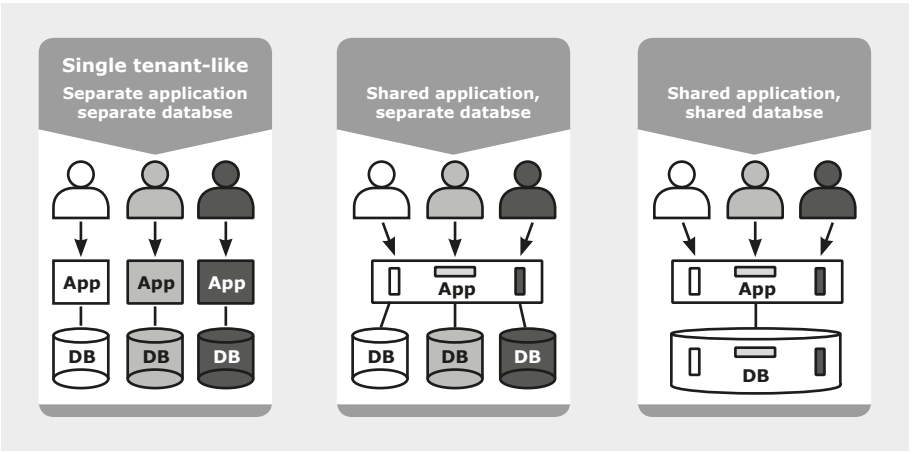

Figura 2 - Modelos de Tenants

7.3.1. Tipos de Tenant

1) Single tenant-like: aplicação e base de dados separadas, cada cliente tem a sua aplicação e base de dados distinta dos demais clientes. Esse modelo favorece aplicações customizadas para cada cliente, com códigos fontes diferentes para cada empresa. Nesse modelo é possível que as mudanças sejam publicadas no ambiente de produção em tempos distintos para cada cliente;

2) Shared application, separate database: todos os clientes acessam a mesma aplicação, porém bases de dados separadas em máquinas separadas. Nesse modelo, as mudanças e novas versões devem ser publicadas no ambiente de produção para todos os clientes ao mesmo tempo;

3) Shared application, shared database: todos os clientes acessam a mesma aplicação e a mesma base de dados. A estrutura da base é a mesma, mas deve ser garantido que cada registro é específico do seu cliente, com uma seção do banco de dados separada para cada empresa. Nesse modelo, as mudanças e as novas versões devem ser publicadas no ambiente de produção para todos os clientes ao mesmo tempo. Conforme a aplicação se torna mais conhecida e utilizada por vários clientes e muitos usuários, o fornecedor tende a distribuir a demanda do banco de dados em máquinas diferentes, podendo passar o tipo de tenant para o modelo anterior (Shared application, separate database).

As indústrias de Ciências da Vida devem buscar por aplicações que armazenem os dados de seus processos de forma segura, e que os dados de uma empresa não estejam disponíveis para outras companhias. Dessa forma, buscam-se:

1) Integridade/veracidade de dados;

2) Privacidade de dados.

Sabemos que existem aplicações em nuvem que não trabalham com estrutura multi-tenants, por exemplo: e-mails, suítes de aplicativos corporativos etc., porém bancos de dados separados ou seções de bancos de dados separadas para cada cliente contribuem para a privacidade de dados e deve ser considerado para sistema SaaS BPx relevante.

O processo de qualificação do fornecedor de SaaS deve incluir o entendimento de tipos de tenants, exemplos:

1) Funcionalidades especiais que estão sendo desenvolvidas especificamente para a empresa regulada;

2) Utilização da mesma aplicação para todos os demais clientes;

3) Mesma aplicação, porém, os dados armazenados em banco exclusivo para o cliente.

O mais importante em qualquer modelo é certificar-se de que o fornecedor garante a privacidade dos dados armazenados. Para o fornecedor que trabalha no modelo shared application, shared database, deve-se solicitar dados,

informações e testes que garantam que os dados são exclusivos do cliente, e que os dados de uma empresa não ficarão disponíveis para outra empresa.

7.3.2. Estratégia de Validação por tipo de Tenant – Fornecedor

Os tipos de tenant que utilizam a mesma versão do sistema para clientes diferentes (prateleira) deveriam possuir a boa prática de validar o sistema internamente. Caso o fornecedor seja bem estabelecido no mercado de Ciências da Vida e comprovar que utiliza boas práticas, pode ser suficiente que o cliente audite a documentação elaborada pelo fornecedor de forma a certificar-se que todos os testes de todas as funcionalidades foram realizados.

Essa abordagem pode otimizar tempo e custo, reduzindo até a realização de testes de qualificação de instalação e operação nas instalações do cliente. Testes de desempenho focados principalmente nas parametrizações específicas para a tenant em questão pode ser uma abordagem robusta.

A auditoria do fornecedor de SaaS deve ser documentada.

A cada controle de mudança e novas versões dos documentos do fornecedor, esses devem ser disponibilizadas ao cliente.

Qualificação de Serviços de Infraestrutura e *Softwares* em Nuvem

8. Qualificação de Serviços de Infraestrutura e *Softwares* em Nuvem

A avaliação dos provedores de serviço em nuvem é uma etapa crítica e deve ser realizada antes da sua utilização, por isso se faz necessário atribuir requisitos mínimos para que eles atendam às especificações de qualidade designadas pela empresa.

Antes de começar a etapa de seleção de provedores é importante verificar os aspectos dos países em que há intenção de utilizar o serviço.

8.1. Seleção do País onde os Dados serão Hospedados

O BSA (Business Software Alliance) emite o relatório BSA Global Cloud Computing Scorecard (Bsa Global Cloud Computing Scorecard [2019]. Disponível em: <https://cloudscorecard.bsa.org>. Acesso em 26 fev. 2019, o qual tem como objetivo avaliar questões relevantes para a seleção do provedor de serviços em nuvem a depender do país onde o provedor está localizado.

8.2. Questionário para Seleção do Provedor

Para certificar que o provedor avaliado atenda a todos os requisitos mínimos pré-estabelecidos pela empresa contratante, recomenda-se que o mesmo esteja em conformidade com o questionário do CSA (Cloud Security Alliance). Os questionários submetidos para o CSA pelos provedores de serviços em nuvem podem ser verificados no Star Registry [2019], disponível em: <https://cloudsecurityalliance.org/star/registry>. Acesso em: 26 fev. 2019. É importante ressaltar que a responsabilidade da avaliação do questionário, a fim de garantir o atendimento dos requisitos mínimo é da empresa contratante.

Caso o provedor não tenha respondido o questionário do CSA e não comprove, através de certificações (ex. ISO 27001, 27002, 27017, 27018), que atende a todos os requisitos de segurança e privacidade que afetam a qualidade do produto, esse provedor deve responder a um questionário elaborado pela empresa contratante.

Esse questionário deve abordar todos os itens relevantes para a avaliação do provedor e pode ser preenchido pelo próprio provedor ou por um responsável designado pela empresa contratante. Para a elaboração desse documento, as perguntas dispostas no questionário do CSA podem ser utilizadas. O questionário do CSA pode ser consultado no Consensus Assessments Working Group [2019]. Disponível em: <https://cloudsecurityalliance.org/working-groups/consensus-assessments/#_overview>. Acesso em 26 fev. 2019.

Observação: O preenchimento do questionário não restringe a busca por outras informações do provedor relevantes para o serviço a ser contratado, que não estejam expressas na planilha do CSA.

8.3. Análise da Avaliação do Provedor

A partir da análise do questionário do provedor (CSA ou empresa) elabora-se

um racional com os fatores e as justificativas que levaram à aprovação e consequente escolha do provedor.

8.4. Contrato - Empresa e Provedor

Recomenda-se estabelecer as diretrizes contratuais do provedor, respondendo, pelo menos, os itens abaixo:

1) Qual o propósito do contrato?
2) Quais serão as responsabilidades do cliente (empresa contratante) no controle de dados e do provedor no processamento dos dados?
3) Qual será o nível de serviço (SLA) estabelecido em contrato?
4) Como será definido o acordo de confidencialidade entre as partes?

Caso as questões acima não sejam respondidas através do contrato, é recomendável verificar em qual documento as respostas podem ser encontradas.

A ferramenta (questionário) é válida e útil na avaliação do provedor para identificação de possíveis riscos e propostas de ações que possam ser estabelecidas em contrato, caso aplicável.

8.5. Qualificação de Infraestrutura e Validação do Sistema SaaS

Após a finalização do processo de avaliação e seleção do provedor de serviços em nuvem é iniciado o ciclo de qualificação e/ou validação.

O questionário de avaliação do provedor, proveniente da CSA ou elaborado pela empresa contratante, dará suporte na elaboração dos documentos iniciais do ciclo de vida, como por exemplo, a Especificação de Requisitos do Usuário e a Análise de Riscos. As questões presentes no questionário devem ser convertidas em requisitos e riscos, respectivamente.

Requisitos e riscos adicionais, pertinentes ao sistema ou infraestrutura, foco do trabalho de validação/qualificação, devem ser incluídos nestes documentos, garantindo assim maior robustez da documentação.

8.5.1. Qualificação de Infraestrutura

Para a realização da qualificação da infraestrutura (IaaS e PaaS) a segunda edição do guia do ISPE, IT Infrastructure Control and Compliance, publicada em 2017, pode ser utilizada como fonte de consulta.

Exemplos de IaaS (infraestrutura como serviço):

Sistemas Operacionais, Servidores, Máquinas Virtuais, Serviços de Armazenamento, Dispositivos de Segurança, Firewalls de Rede, Data Centers etc. A AWS (Amazon Web Services) e a Microsoft Azure são exemplos de IaaS comercializados atualmente.

Exemplos de PaaS (plataforma como serviço):

Ferramentas de desenvolvimento, testes e implementação de aplicações,

gerenciamento de banco de dados, análise de negócios, hospedagem de sites etc. O Red Hat Open Shift e o Google app Engine são exemplos atuais de PaaS.

8.5.2. Validação de Sistemas Computadorizados

Para a validação de sistemas disponibilizados através do modelo SaaS (software como serviço), o guia de Validação de Sistemas Computadorizados da ANVISA, publicado em 2010, pode ser utilizado como base.

Exemplos de Saas:

Office 365, ERP's, provedores de e-mails, aplicações de Gerenciamento de Projetos, mas não limitados a.

Observação: um provedor pode fornecer mais de um tipo de serviço em nuvem. Cabe à empresa contratante estabelecer os requisitos e avaliar qual o provedor e serviço(s) irão atender às necessidades. Logo após a contratação, qualificar e/ou validar o serviço contratado, é importante, pois a responsabilidade regulatória permanece com a empresa contratante.

Segurança da Informação para os Serviços de *Cloud Computing* (Computação na Nuvem)

9. Segurança da Informação para os Serviços de *Cloud Computing* (Computação na Nuvem)

O uso dos serviços de Computação na nuvem (cloud computing) exigem medidas de segurança aplicadas aos processos realizados neste tipo de plataforma, que é cada vez mais utilizada na rotina das empresas. Casos de ataques cibernéticos, ameaças de vírus, dentre outros problemas trazem reflexões na gestão e organização das barreiras de segurança necessárias para a tomada de ações preventivas e corretivas, que podem ser adotadas pelas empresas e pelo provedor do serviço.

Frente a este cenário, indústrias do segmento de Ciências da Vida, como as empresas farmacêuticas, estudam a melhor forma de lidar com esse assunto crucial frente as BPx e as agências regulatórias (nacionais e internacionais). Na rotina dessas empresas, os departamentos de TI e Garantia da Qualidade/ Validação buscam de forma documentada avaliar e testar as funcionalidades do serviço, e dentre elas os quesitos de segurança são tidos como pontos críticos a serem avaliados. Dessa forma, a implementação e uso dos controles de segurança na nuvem, seguem diretrizes tanto para o usuário/cliente como para o provedor do serviço/fornecedor baseados em uma análise de riscos que avalia as implicações legais, contratuais, regulatórias e de interesse do negócio.

9.1. Conceitos Gerais de Segurança da Informação

Os princípios da segurança da informação – **disponibilidade, integridade, confidencialidade e autenticidade** também são aplicados ao ambiente de cloud, considerando as particularidades da nuvem.

A **integridade** consiste na manutenção dos dados na forma como foi concebida e armazenada, de modo que apenas pessoas autorizadas tenham acesso e condições de modificar as informações.

Nota: sistemas on-premisses com dados que podem ser alterados por usuários da TI ou do negócio da contratante que não deixam rastro da modificação somada às mudanças não controladas, não são validáveis pela falta de comprovação de integridade de dados. A utilização do mesmo sistema hospedado em nuvem no modelo SaaS administrado pelo fornecedor pode ser uma opção devido à vedação dos usuários da contratante não possuírem acesso às tabelas do banco.

A **disponibilidade** das informações consiste em seu acesso eficaz no momento em que forem requisitadas, de modo que os processos não sejam prejudicados pela operacionalidade do ambiente de cloud.

A **autenticidade** consiste na conferência da entrada e da operação dos dados, garantindo que apenas aqueles que possuem autorização realizem as atividades junto ao ambiente de cloud.

A **confidencialidade** consiste no acesso às informações por usuários autorizados, sendo essa garantida pelo controle de acesso/autenticação.

9.1.1. Gerenciando os Riscos de Informação nos Serviços de Cloud (Serviços de Nuvem)

No ambiente de computação na nuvem, os dados dos usuários/clientes são armazenados, transmitidos e processados pelo provedor do serviço. Dessa forma, caso não haja os controles necessários sobre o serviço, o usuário/cliente precisará tomar precauções extras com as práticas de segurança da informação. Assim, antes que seja estabelecida a contratação de serviços de cloud, o usuário deve levar em consideração os requerimentos de segurança necessários a este *versus* a capacidade do provedor de atender tais requisitos. Deve-se também avaliar a possibilidade de gerenciamento das configurações de segurança pelo usuário para o uso da plataforma, e a análise dos riscos que permite verificar as vulnerabilidades e assim tomar as ações necessárias para o gerenciamento de segurança como um todo.

9.1.2. Relação entre os Serviços de Cliente na Nuvem (Cloud Service Customer) e Serviços dos Provedores na Nuvem (Cloud Service Providers)

O provedor/fornecedor de serviços de computação na nuvem e o cliente/usuário (Serviço de Cloud ao Cliente) devem possuir o processo de gerenciamento de riscos implementados, a fim de auxiliar no entendimento e gerenciamento dos riscos associados a aplicação dos serviços na nuvem.

Em contraste com a aplicação geral do processo de gerenciamento de riscos de segurança da informação, a computação na nuvem possui seus próprios riscos específicos, alguns exemplos:

1) Uso do trabalho em rede (network);
2) Ambiente de compartilhamento;
3) Serviço de auto provisionamento (cliente/usuário pode provisionar por conta própria recursos de computação, como tempo de servidor e armazenamento em rede, automaticamente, e conforme necessário, sem necessitar intervenção humana dos provedores de serviços de nuvem);
4) Administração sob demanda;
5) Ambiente virtual, limitado à visibilidade da implementação de controles físicos. Desse modo, faz-se necessária a verificação das certificações do provedor, como por exemplo, a ISO 27001, no processo de qualificação do fornecedor de infraestrutura;
6) Serviços utilizados/prestados por fornecedores de países diferentes – leis locais devem ser avaliadas, a fim de se garantir a privacidade e segurança das informações que são trabalhadas junto da computação na nuvem.

9.1.2.1. BSA Global Cloud Computing Scorecard

BSA Software Alliance é uma associação com sede em Washigton, DC, com presença em mais de 60 países que possui membros que desenvolvem e comercializam softwares e juntos trabalham para combater pirataria e ataques cibernético, promovendo segurança da informação.

Anualmente ocorre o BSA Global Cloud Computing Scorecard, o qual promove um ranking dos países em termos de qualidade de prestação de serviços na nuvem. São avaliados os seguintes critérios:

1) Privacidade de dados: avalia e acompanha como os países em suas particularidades estabelecem as diretrizes para tratar os dados privados, bem como os avanços independentes ao apresentarem legislações mais abrangentes;

2) Segurança: avalia e acompanha como os países regulam cyber segurança, certificação e testes;

3) Crimes cibernéticos: avalia as leis que regem os crimes cibernéticos, as investigações e as penalidades;

4) Direitos de propriedade intelectual: avalia e acompanha como os países tratam dos assuntos pertinentes à propriedade intelectual;

5) Padrões e harmonização internacional: avalia e acompanha como os países regulam o comércio digital, suas tarifas e barreiras de comércio;

6) Promoção do livre comércio: avalia e acompanha os regimes governamentais quanto à existência de barreiras, esforços para padronizar e realizar o livre comércio;

7) Infraestrutura de TI e desenvolvimento de banda larga: avalia a capacidade dos países em fornecer infraestrutura necessária para a adequada operação dos serviços em nuvem.

Em 2018 foram avaliados 24 países, dos quais os 5 primeiros que obtiveram as maiores pontuações foram: Alemanha, Japão, Estados Unidos, Reino Unido e Austrália, sendo, portanto, os locais mais indicados para comportar as instalações de infraestrutura de cloud. É importante ressaltar que as avaliações são realizadas considerando uma série de critérios diferentes e que dependendo da necessidade da empresa, o ranking geral pode não ser o melhor critério.

9.2. Política de Segurança da Informação

Para a realização de atividades na nuvem é necessário que haja uma política de segurança da informação que aborde os tópicos relacionados à plataforma de cloud, atentando-se para as particularidades relacionadas ao prestador de serviço e ao usuário. Ambos possuem ações de segurança que precisam ser empregadas em conjunto, a fim de se garantir o ambiente seguro.

9.2.1. Cloud Service Customer (Usuário do Serviço de Nuvem)

Os usuários de serviço de cloud (clientes) devem ter uma política de segurança da informação que se atente aos itens de cloud, nos seguintes pontos (mas não limitados a):

1) Informações armazenadas em cloud podem ser acessadas e gerenciadas pelo provedor de serviço na nuvem;

2) Processos podem ocorrer em múltiplas locações compartilhadas nos mesmos servidores, onde as informações podem ser armazenadas com segurança de separação lógica (virtualização);

3) Os usuários de serviço na nuvem e a criticidade do uso;

4) Os administradores de serviço de cloud (internos da empresa do usuário) que possuem acessos privilegiados;

5) A localização geográfica da organização do provedor do serviço de cloud e os países (e estado) onde o provedor do serviço pode armazenar os dados do cliente, mesmo que temporariamente (é interessante que o provedor esteja localizado em local com leis robustas, conforme BSA o qual avalia a segurança da informação com base na localização geográfica, entre outros tópicos – veja mais detalhes no item "Seleção do País onde os Dados serão Hospedados";

6) Tem de haver acordo/contrato em que o provedor e usuário concordam com os termos de segurança da informação.

9.2.2. Cloud Service Provider (Provedor de Serviço na Nuvem)

O provedor de serviços em cloud deve aplicar as políticas de segurança da informação, levando em consideração:

1) Os requerimentos de segurança da informação e riscos entendendo as particularidades de cada segmento;

2) Múltiplas locações (posições) e isolamento de serviços na nuvem para clientes (inclui virtualização ou tenants);

3) O provedor de serviços deverá ter procedimentos estabelecidos e equipe treinada para disponibilizá-los de forma apropriada sem invadir a privacidade dos dados dos usuários e/ou dos processos das empresas;

4) Procedimentos de controle de acesso, por exemplo: autenticação forte (duplo fator, tokens, senhas complexas etc.) para acesso dos administradores junto aos serviços de cloud;

5) Comunicação eficiente e prévia da aplicação de mudanças junto à plataforma de cloud ao cliente/usuário;

6) Segurança com relação à virtualização dos ambientes compartilhados;

7) Gerenciamento do ciclo de vida das contas do cliente/usuários;

8) Definir as políticas de comunicação de violações e compartilhamento de informações (vazamentos) e respectivos planos de ações de incidente;

9) Deve prover um canal de comunicação/assistência entre o provedor de serviço e o cliente/usuários do serviço de cloud. Sendo o caso, tem de ser determinado um prazo para os atendimentos e respostas a quaisquer solicitações do cliente.

Os provedores de serviço em cloud devem seguir as diretrizes de segurança da informação do segmento e afins, tais quais:

A família das ISO 27000 relacionadas à segurança da informação, da qual se destacam as:

- ISO 27001:2013 Information technology - Security techniques - Information security management systems - Requirements;
- ISO/IEC 27002:2013, Information technology - Security techniques - Code of practice for information security controls;
- ISO/IEC 27018:2014 Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;

Uma vez instaurada as diretrizes internas do fornecedor e/ou diretrizes de mercado, das políticas de segurança, os provedores de cloud podem se submeter a avaliações de instituições que os certificam. Alguns exemplos dessas instituições são:

- Cloud Security Alliance (CSA [2018]. Disponível em: <https://cloudsecurityalliance.org/>. Acesso em 01 nov. 2018.): é uma organização sem fins lucrativos que promove as melhores práticas de segurança para os serviços em cloud. A entidade certifica a empresa prestadora de serviços em nuvem e profissionais que atuam na área;
- NIST National Institute of Standards and Technology - aplicação da FIPS 140-2 Federal Information Processing Standard: norma que cobra os padrões de criptografias seguras;
- Multi-Tier Cloud Security (MTCS) Singapore Standard (SS) 584: certifica quanto à segurança dos serviços em cloud para a Singapore Info-communications Media Development Authority (IMDA). Foi o primeiro padrão estabelecido considerando as múltiplas camadas de segurança para o segmento de cloud;
- EXIN Cloud Computing Foundation (EXIN Cloud Computing Foundation. [2018]. Disponível em:<https://www.exin.com/certifications/exin-cloud-computing-foundation-exam?language_content_entity=pt-br>. Acesso em 01 nov. 2018.): certifica os fornecedores de serviço em cloud no nível operacional (certificações de profissionais);
- Federal Risk and Authorization Management Program (FEDRAMP [2018]. Disponível em: <https://www.fedramp.gov/>. Acesso em 01 nov. 2018.): programa federal de gerenciamento e autorização de risco do governo dos Estados Unidos para avaliação de segurança, autorização e monitoramento contínuo de produtos e serviços na nuvem. No caso, os serviços têm de seguir a Lei Federal de gerenciamento da segurança da informação (FISMA – Federal Information Security Management Act). No caso, os prestadores de serviço em cloud são avaliados por uma organização externa de avaliação - Third Party Assessment Organizations (3PAOs).

Além das diretrizes de políticas de segurança, é importante que os provedores de cloud sigam as diretrizes internacionais de segurança na nuvem, conforme a UK National Cyber Security Centre (Cloud security

guidance. [2018]. Disponível em: <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>. Acesso em 01 nov. 2018.), a qual define a aplicação dos 14 princípios de cloud security. Seguem os princípios:

1) Proteção dos dados em trânsito: os dados em trânsito devem ser adequadamente protegidos contra adulterações e interceptações;

2) Os dados do usuário e os ativos que o armazenam ou processam devem ser protegidos contra adulteração física, perda, dano ou apreensão;

3) Separação entre usuários: um usuário mal-intencionado ou comprometido do serviço não deve conseguir afetar o serviço ou os dados de outro usuário;

4) Estrutura de governança: o provedor de serviços deve ter uma estrutura de governança de segurança que coordene e direcione seu gerenciamento do serviço e das informações nele contidas. Quaisquer controles técnicos implantados fora dessa estrutura podem ser prejudicados;

5) Segurança Operacional: o serviço precisa ser operado e gerenciado com segurança para impedir ou detectar ataques. Deve haver equilíbrio entre operação e implementação de ações contra ataques cibernéticos de forma que garanta segurança operacional, sendo ainda viável economicamente para o negócio. Estratégias documentadas baseadas em riscos devem ser utilizadas;

6) Segurança Pessoal: quando os prestadores de serviço do provedor possuem acesso aos dados e sistemas, há a necessidade de ter alto grau de confiabilidade apoiado por treinamento adequado, reduzindo a probabilidade de comprometimento acidental ou mal-intencionado pelos profissionais da empresa prestadora de serviços;

7) Desenvolvimento seguro: os serviços devem ser projetados, e desenvolvidos para identificar e mitigar ameaças à sua segurança do cliente e/ou do próprio provedor. Os serviços que não atendem regras de desenvolvimento seguro podem estar sujeitos a vulnerabilidades e problemas de segurança que podem comprometer dados, causar perda de serviço ou ser suscetível a outras atividades mal-intencionadas;

8) Cadeia de suprimentos de segurança: o provedor de serviços deve garantir que sua cadeia de suprimentos atenda satisfatoriamente a todos os princípios de segurança que o serviço alega implementar;

9) Gerenciamento seguro de usuários: o provedor deve disponibilizar as ferramentas para o gerenciamento dos usuários com segurança. As interfaces e procedimentos de gerenciamento são uma parte vital da barreira de segurança, impedindo o acesso não autorizado e a alteração de seus recursos, aplicativos e dados;

10) Identidade e autenticação: todo o acesso a interfaces de serviço deve ser restrito a indivíduos autenticados e autorizados;

11) Proteção de interface externa: todas as interfaces externas ou menos confiáveis do serviço devem ser identificadas e adequadamente protegidas;

12) Administração de serviço: os sistemas usados para administração de um serviço de cloud normalmente possuem acesso altamente privilegiado. Seu comprometimento no uso adequado possui impacto significativo, incluindo os meios de ultrapassar métodos de segurança e assim sequestrar ou manipular dados;

13) Auditoria da informação: o serviço de cloud deve ser capaz de prover auditorias (audit trails) necessárias para monitorar o acesso ao serviço e as atividades realizadas nele. O tipo de informação obtida através da realização de auditorias é importante para a sua capacidade de detectar e responder a atividades impróprias ou mal-intencionadas;

14) Uso seguro do serviço: a segurança dos serviços em cloud e os dados contidos neles podem ser prejudicados se o serviço for utilizado de maneira inadequada. Consequentemente, há responsabilidades no uso do serviço para que os dados sejam adequadamente protegidos por parte do cliente (responsabilidade compartilhada).

9.2.3. Revisão de Políticas para Segurança da Informação

Periodicamente a política de segurança da informação tem de ser revisitada por ambos (provedor e cliente) tendo em vista as constantes atualizações referentes ao tema e as possíveis melhorias que podem ser incluídas.

9.3. Infraestrutura

A segurança da informação aplicada à plataforma em cloud inclui infraestrutura como uma das premissas para o bom desempenho de seu uso. No caso, um design adequado desta infra interferirá em todo o ciclo de vida das informações armazenadas em nuvem.

A segurança da infraestrutura possui várias camadas de proteção, das quais pode-se destacar a segurança operacional, a comunicação via internet, os serviços de armazenamento, a autenticação de usuários, a implantação dos serviços de cloud e a infraestrutura de hardware.

9.3.1. Infraestrutura de Hardware

Os dados/informações que são administrados pelo uso da plataforma em cloud estão fisicamente armazenados em servidores localizados em data centers. Os data centers são instalações físicas normalmente de acesso restrito, protegidos com o uso de identificação biométrica e/ou outras tecnologias de identificação, bem como sistemas de detecção de intrusos. Os servidores são concebidos de forma segura e podem ser acompanhados durante a sua instalação de modo a ter os componentes de hardware autenticados. Outro ponto de segurança importante é a inicialização dos servidores (opera-

cionalidade), bem como a realização de eventuais atualizações com o uso de assinaturas criptografadas. Os servidores são monitorados a fim de estarem atualizados quanto as suas versões (incluindo patches de segurança), para detectar eventuais problemas de hardware ou software, que podem significar eventuais manutenções.

9.3.2. Implantação do Serviço – Escopo do Provedor (transparência para o Usuário Final)

A equipe do projeto e suas responsabilidades podem variar de acordo com o tipo e finalidade do serviço adquirido e/ou procedimentos internos do cliente final. Contudo, recomenda-se que tais responsabilidades sejam bem definidas no início do projeto e que a implementação seja multidisciplinar.

Durante a implantação do serviço de cloud, deve ser utilizada autenticação criptografada para estabelecer a comunicação entre servidores, bem como o uso de pontos de filtragem de entrada e saída em diferentes pontos da rede, a fim de impedir falsificações de IP (Internet Protocol). Podem ser geradas credenciais criptografadas que garantem a comunicação com o servidor correto. Podem ser também utilizadas camadas de isolamento de modo a proteger serviços distintos na mesma máquina (ex: virtualização, separação do usuário de Linux, linguagem), e podem ser utilizadas máquinas dedicadas (para dados com alto grau de confidencialidade). A rede interna de comunicação (LAN – Local Area Network) entre servidores pode ser criptografada de modo a dar segurança caso ocorra alguma interferência na rede.

A virtualização que permite a segregação virtual entre diferentes usuários é realizada por um sistema que implanta e permite a gestão da aplicação na forma de containers. Para as operações que trabalham em ambiente compartilhado, existem controles de segurança que os próprios fornecedores podem oferecer ou trabalhar com outras empresas que monitoram, identificam vulnerabilidades, emitem alertas, bloqueiam anomalias, e até mesmo interrompem ataques.

9.3.3. Armazenamento Seguro dos Dados – Responsabilidade do Provedor

O armazenamento em cloud pode apresentar várias configurações seguras de armazenamento, sendo que os dados podem estar em diferentes condições. Os dados podem passar por criptografia antes de serem armazenados, de modo a ter maior segurança das informações em caso de ocorrência de acesso inadvertido, dessa forma, os dados continuarão seguros. Com os dados criptografados, eles podem ser devidamente armazenados fisicamente em discos rígidos (hard disk – HD ou solid-state drive - SSD) dos servidores, por exemplo.

O armazenamento seguro dos dados também envolve a aplicação de redundância nos locais de armazenamento, de forma que seja possível a recuperação eles em situação de desastre, e/ou solicitação de recuperação, caso o dado seja apagado de forma indevida pelo cliente. É válido ressaltar que vários provedores de cloud já oferecem a redundância na replicação de

dados, inclusive aplicando a redundância geográfica, de modo a permitir a recuperação segura em casos de desastre.

A exclusão de dados pelo cliente de forma indevida e/ou errônea é um item que pode ser mencionado na política de segurança para contratação do serviço de cloud. Assim, para manutenção dos dados indevidamente excluídos, é importante que o usuário tenha ciência do prazo de deleção definitiva de tais dados no provedor.

Após o fim do contrato de serviço em nuvem, no momento de descomissionamento total dos dados, o provedor deve confirmar a deleção da base de dados do cliente. Recomenda-se um planejamento adequado da fase de descomissionamento. Sugerimos o Guia GAMP 5: A Risk-based Approach to Compliant GxP Computerized Systems para a definição de uma abordagem documentada.

9.3.4. Comunicação Segura com a Internet – Exemplos de Gerenciamentos por parte do Provedor e Cliente

As comunicações devem ser aplicadas com o uso de protocolos de segurança certificados via internet de forma segura.

É comum, nesta via, ataques que visam a interrupção do serviço das páginas do usuário ao sobrecarregar os servidores de internet. Assim, por meio de um ataque sincronizado simultâneo de várias máquinas, há a sobrecarga do serviço, em que este se torna incapaz de realizar suas atividades, visto que não é possível processar o volume de dados gerados. Dessa forma, o usuário não consegue executar suas atividades, uma vez que a rede está inundada. Para que o usuário não sofra com esse tipo de ataque, é válido contar com os serviços dos grandes provedores, pois esses possuem infraestrutura adequada para suportar ataques dessa natureza. Esses grandes provedores são capazes de monitorar o tráfego de suas redes e os acessos, e ao detectarem um pico anômalo, conseguem restringir e filtrar os acessos maliciosos, de modo que esses não comprometam a operacionalidade do provedor de cloud para o usuário final.

Assim, é importante que o acesso via internet aos serviços dos provedores seja baseado em controles de acesso por meio de autenticações, garantindo que apenas usuários devidamente cadastrados acessem os serviços de cloud. As autenticações normalmente são baseadas no uso de login e senha, bem como a aplicação de ferramentas adicionais de identificação, como o envio de senhas adicionais por meio de celulares e aplicativos e uso de tokens. De qualquer forma, recomenda-se que seja responsabilidade do usuário da infraestrutura e/ou usuário da aplicação, que utilize pelo menos duas formas de autenticação ou multi-fator (MFA Multi Factor Authentication). Recomenda-se ainda que dispositivos que auxiliam na geração de autenticação de multifator sejam criptografados.

9.3.5. Gerenciamento de Identidade e Acesso - Responsabilidade do Cliente

Os dados em cloud precisam de forte controle de acesso e hierarquia para as operações realizadas na plataforma. Para tal, apenas usuários autorizados

podem ter acesso às funções de configuração, edição e criação/exclusão de dados e configurações dos servidores. Assim, junto à função de operação, é possível aplicar bloqueios de funcionalidades/telas/senhas, exclusões de usuários/grupos, que permitem definir regras para autorizar o gerenciamento dos sistemas pelos diferentes níveis de usuários.

9.3.6. Trilha de Auditoria (Audit Trail) nos Serviços de Infraestrutura

Grandes e estruturados provedores de nuvem possuem a funcionalidade que possibilita governança, conformidade, auditoria operacional e auditoria de riscos no serviço de nuvem. Normalmente é possível registrar, monitorar continuamente e reter a atividade da conta relacionada às ações executadas na infraestrutura. Assim, tal funcionalidade disponibiliza o histórico de eventos da atividade da conta, inclusive ações executadas por meio do Console de Gerenciamento e das ferramentas da linha de comando e de outros Serviços do provedor. Esse histórico de eventos simplifica a análise de segurança, o rastreamento de alterações de recursos e a solução de problemas. Dessa forma, recomenda-se verificar se não é possível a deleção da trilha de auditoria e/ou sua modificação.

9.3.7. Segurança de Rede

A segurança da rede aplicada aos serviços de cloud possui suas ações no trânsito seguro de informações entre os usuários e os provedores. Muitas empresas, para garantir o acesso restrito à rede, fazem uso da nuvem privada, de modo a evitar o trânsito de informações pela internet pública. Os serviços de nuvem privado muitas vezes contam com uma rede expansível (elástica) que permite o crescimento da estrutura conforme a necessidade da empresa, sem impactos nos processos, visto que este crescimento não causa interrupções ou inatividades para o usuário. Para as redes usadas no serviço de cloud, é comum implantar sistemas de monitoramento, que buscam pontos de fragilidade e otimização de processo. Esses monitoramentos podem ser periódicos quando programados pelo cliente no serviço de cloud.

Durante o fluxo de atividades das operações: alterações de usuários, tráfego de rede (volume de informações), realização de backups, e outras condições, o balanceamento de rede é necessário, de modo a otimizar os processos em andamento. Nesse caso, o tráfego é direcionado para outras regiões físicas ou virtuais e permite a continuidade do processo, de modo a não ser afetado pela alta demanda de serviços. Esse trabalho pode ser realizado tanto pelo provedor de serviços como pelo cliente final, dependendo do projeto.

Recomenda-se que a segurança das informações disponibilizadas no serviço de cloud estejam protegidas pela criptografia dos dados, podendo ser: em repouso, em trânsito ou em uso. Abordagem baseada em risco conduzida pelo fornecedor pode justificar eventual ausência ou necessidade de criptografia.

9.3.8. Segurança Operacional – Provedores e Clientes

A operacionalidade dos serviços de cloud está relacionada à forma como os fornecedores desse tipo de serviço investem em sua infraestrutura. Assim,

empresas desse segmento investem tanto no desenvolvimento de softwares de gerenciamento da arquitetura do sistema de forma automatizada e de contínuo desenvolvimento quanto na aplicação de revisões periódicas das programações, que detectam eventuais bugs de segurança. Além disso, contam com bibliotecas de linhas de programação que impedem que desenvolvedores apliquem programações que no passado apresentaram falhas ao serem aplicadas.

Como forma de atestar a segurança de suas aplicações em cloud, é interessante que tanto provedores quanto clientes gerenciem periodicamente riscos cibernéticos dos seus servidores, inclusive com o uso de aplicações automatizadas que simulam condições aleatórias a fim de evidenciar falhas/vulnerabilidades com às operações. As vulnerabilidades podem ser conferidas nos bancos de dados da CVE (Common Vulnerabilities and Exposures [2018]. Disponível em: <https://cve.mitre.org/about/index.html>. Acesso em 01 nov. 2018.).

Além disso, é importante que provedores de serviço em cloud e clientes monitorem internamente os seus funcionários e suas ações com à operacionalidade das atividades em cloud. Assim, é comum a prática da realização do monitoramento das ações dos profissionais, bem como a realização de auditorias periódicas. É comum também a intensificação dos treinamentos aos colaboradores na área de segurança da informação, a fim de melhorar seu comportamento no uso dos sistemas de forma a evitar, por exemplo, práticas de phishing, que se refere à tentativa de roubo de credenciais para acessos mal-intencionados.

Backup e Recovery na Nuvem

10. Backup e Recovery na Nuvem

10.1. Importância do Backup nas Organizações

Diante do avanço tecnológico com o uso de computadores, automação do chão de fábrica e toda a rotina de documentação ser de origem eletrônica, tais ativos tornaram-se essenciais para o andamento e tomada de decisões nas organizações, sendo primordial mantê-las seguras. É incontável a quantidade de registros, arquivos, mensagens e documentos que circulam diariamente pela rede corporativa, que são compartilhados e que podem estar expostos a diversos riscos, como falhas nos servidores, roubos, vazamentos, perdas e arquivos corrompidos, além de se tornarem alvos de diversos ataques direcionados. Normalmente, esses problemas ocorrem devido às paradas, falhas, invasões e interrupções na rede e nos servidores, de modo a atingir diretamente a produtividade de toda a empresa e muitas vezes causar prejuízos imensuráveis.

Sendo assim, é importante contar com uma solução de backup para garantir a disponibilidade de todos os dados, garantindo que, independentemente de falhas técnicas, acidentes ou paradas, suas informações estarão redundantes em um local seguro. O backup, em suma, é uma ferramenta no nível de negócio, que é sinônimo de proteção de dados, segurança da informação e integridade de dados.

10.2. Consideração Importante: Diferença entre Armazenamento e Backup na Nuvem

O armazenamento em nuvem é um serviço de guarda de arquivos, que tem como objetivo proteger os dados eletrônicos de falhas em equipamentos físicos, formatações, queima, exclusões, quebra, entre outros. Esse serviço permite a inserção de todos os arquivos na nuvem e que esses fiquem disponíveis em qualquer dispositivo com acesso à internet, como smartphones e tablets. Porém, é válido ressaltar que durante o armazenamento dos dados, não há a criação de cópias desses arquivos, mas apenas a sua centralização em um servidor online. Assim, caso seja excluído um arquivo na nuvem, esse arquivo deixará de existir em qualquer dispositivo, sem possibilidade de recuperação. Todos os usuários que estão sincronizados com o mesmo arquivo excluído, também não terão mais acesso a ele.

Em caso de armazenamento de dados (archive) em nuvem, não significa que o backup dos dados está sendo feito automaticamente. Deve ser definida a estratégia e configurada a ferramenta de backup que pode ocorrer também na nuvem ou a sua utilização quando os dados são armazenados localmente. A responsabilidade por configurar ou definir a política de backup é da empresa contratante.

10.3. Tipos e Formas de Backup

Atualmente, as organizações podem adotar como estratégia dois tipos de backups: tradicionais (físicos) e em nuvem.

Os backups tradicionais geralmente são feitos através de servidores físicos, instalados em torres alimentadas por nobreaks industriais capazes de garantir a segurança dos dados mesmo sem energia. Tais backups são adequados para proteção dos dados em casos de exclusão (intencional ou não) de arquivos, falhas de hardware ou software, porém, existem riscos relacionados a desastres naturais (incêndios, inundações etc.); e roubo ou sabotagem de dispositivos (fitas físicas). Além disso, outras desvantagens do backup tradicional é o alto custo de aquisição, estrutura e manutenção.

Quanto aos backups na nuvem, estes passaram a ser uma solução eficaz e praticamente indispensável para os mais variados tipos de organização, visto que são mais acessíveis e mais rápidos para serem restaurados, e mais confiáveis, sem risco de danos aos dados quando comparados às fitas tradicionais.

É extremamente importante a definição da estratégia de backup a se adotar, de modo que esta ferramenta se adeque aos objetivos da organização e, principalmente, cumpra com sua função: garantir ao máximo a segurança dos dados armazenados.

10.4. Backup na Nuvem

Caso a organização opte por realizar o backup na nuvem, busque considerar os fornecedores que prestam esse serviço – disponibilização de um servidor –, que atendam os itens mínimos de contrato conforme o item 'Contrato de Aplicações em Nuvem', disposto neste guia.

Conforme mencionado anteriormente, os backups em nuvem são mais competitivos e mais adequados à realidade atual nas grandes organizações. Além das vantagens já mencionadas, pode-se citar, desde que configuradas pelo contratante:

1) Acessibilidade contínua e restauração rápida: os backups na nuvem sempre são acessíveis, de modo que colaboram para que as restaurações sejam mais rápidas, reduzindo assim, o tempo de inatividade do sistema;

2) Escalabilidade: paga-se apenas pelo espaço consumido na nuvem, além da ilimitada capacidade de armazenamento;

3) Redundância: os dados de backup são armazenados e replicados geograficamente para manter cópias dos seus dados em outros data centers, aumentando a confiabilidade do dado quando armazenamento na nuvem;

4) Segurança: dispõe de camadas de segurança e chaves de criptografia automática, permitindo que seus dados sejam copiados para a nuvem e restaurados de forma segura, impedindo assim que qualquer um acesse às informações;

5) *Restore*: caso seja necessário realizar a restauração dos dados, o processo pode ser automático e ágil, incluindo alarmes de falhas;

6) Substituição das manutenções e riscos de falhas humanas e/ou técnicas após estabelecido o processo de backup, que passa a ser mantido pelo provedor da nuvem. Um ponto adicional é não ser mais necessária troca de hardware interno periodicamente.

Para um backup na nuvem utiliza-se um servidor, o qual disponibiliza um aplicativo que permite o uso do link de internet para a parametrização da ferramenta. Para tal, é de extrema importância a atuação de especialistas de TI da organização, de modo que definam a parametrização conforme a estratégia de política da empresa. Assim, define-se a frequência do backup, isto é, a parametrização dos horários e a necessidade de disponibilização dos dados armazenados na nuvem, e também a definição do tipo de backup a ser realizado – full (completo), incremental ou diferencial –, de modo tanto a otimizar o funcionamento da ferramenta quanto de agilizar o processo de restauração dos dados de backup. Dessa forma, no horário pré-determinado o aplicativo pode coletar, comprimir, criptografar e transferir os dados para a nuvem.

A respeito da criptografia de acesso à nuvem, é importante observar os itens de contrato e se a empresa fornecedora do serviço de backup possui a opção de acesso à nuvem criptografada. A empresa que oferece esse tipo de serviço torna-se ideal para o negócio, visto que nem mesmo o fornecedor detém a chave de acesso, sendo restrita apenas ao cliente. A criptografia de backups é importante, pois é ela que garante que seus dados permaneçam seguros e protegidos contra qualquer tipo de acesso não autorizado. A empresa contratante, que detém a chave, deve gerenciar para que o código criptográfico em si não seja perdido ou divulgado.

O acesso aos dados de backup de uma empresa usualmente é simples, e pode ser feito a partir de qualquer navegador web, desde que seja realizado por usuário autenticado com senha para acessar os dados. Essa senha deve ser criptografada, única e intransferível.

Existem alguns modelos de contratação do serviço de backup que usualmente é mensal e paga-se pela quantidade de bytes que se utiliza e mantém na nuvem, desde que configurado.

10.5. Plano de Recuperação de Desastre e Recuperação de Dados na Nuvem

Além do backup, que é uma ferramenta extremamente importante para o negócio, a recuperação de dados também é algo essencial para as organizações. Por isso, empresas que se preocupam quanto à inatividade de seus processos, devido à perda dos seus dados e/ou longo período de tempo até a recuperação desses, o contratante deve se preocupar em traçar políticas que atendam à continuidade dos negócios da organização, e que englobam um Plano de Recuperação de Desastre (DRP – Disaster Recovery Plan) robusto para a companhia.

Assim, o DRP é responsável em minimizar as consequências e tomar as medidas para a volta da operação normal em um tempo aceitável, e visa a recuperação enquanto o desastre está em curso. Além disso, o DRP está focado no restabelecimento dos sistemas e infraestrutura de TI, que suportam os processos críticos das empresas após eventos de interrupção.

Dessa forma, é necessário estabelecer adequado DRP junto ao time de TI, Diretoria da organização e a equipe Qualidade para o melhor tempo de resposta para os seguintes requisitos:

1) RTOs (Recovery Time Objective - Objetivo do Tempo de Recuperação): limitam o período de volta no tempo, e definem a quantidade máxima permitida de dados perdidos de uma ocorrência de falha para o último backup válido.

2) RPOs (Recovery Point Objective - Ponto Objetivo de Recuperação): estão relacionados ao tempo de inatividade e representam a quantidade de tempo que leva para se recuperar de um incidente até que as operações estejam disponíveis para os usuários.

Sendo assim, melhor será o DRP. Quanto menor forem tais critérios, de modo que o tempo para recuperação dos dados é menor. Na nuvem, é possível parametrizar esses critérios de modo a otimizar o tempo de recuperação de dados em caso de desastre. Além disso, devido aos dados serem compactados nos backups, a sua recuperação torna-se mais ágil.

Quanto ao restore, a restauração dos dados na nuvem, isto é possível à medida que o contratante estabelece o tempo de retenção dos dados, em que o ideal é optar por serviços de longo prazo. Assim, a restauração dos dados se faz através do acesso aos backups na nuvem por um responsável por gerenciar os serviços da nuvem da empresa contratante, e por fim, a disponibilização dos dados para o usuário. No entanto, é válido ressaltar que se o responsável/usuário excluir dados do backup da nuvem, eles não podem ser recuperados. Se o problema de perda de dados for responsabilidade do contrato, este deve executar o processo de restore.

Responsabilidade entre as Partes: Clientes de Serviço em Nuvem e Provedores de Serviço em Nuvem

11. Responsabilidade entre as Partes: Clientes de Serviço em Nuvem e Provedores de Serviço em Nuvem

No ambiente de computação em nuvem, os dados do cliente são armazenados, transmitidos e processados por um serviço de nuvem. Portanto, os processos de negócios de um cliente de serviço de nuvem estão diretamente relacionados à necessidade de consolidação dos processos de segurança da informação, por isso a relevância no estabelecimento das responsabilidades entre as partes envolvidas no contrato.

As responsabilidades mínimas a serem contidas no SLA ou guia para serviços em nuvem estão descritas na tabela a seguir:

Cliente de Serviço em Nuvem	Provedor de Serviço em Nuvem
Política de Segurança da Informação Deve conter, mas não se limitar à: - Descrever as informações armazenadas no ambiente de computação em nuvem, podendo essas estar sujeitas a acesso e gerenciamento pelo provedor de serviços em nuvem, em documento formal que faça parte da qualificação de infraestrutura; - Informar os ativos mantidos no ambiente de computação em nuvem, por exemplo, programas de aplicativos; - Informar sobre gerenciamento de acessos aos serviços em nuvem; - Informar os administradores de serviços de nuvem do cliente que têm acesso privilegiado; - Informar os locais geográficos da organização do provedor de serviços em nuvem e os países em que o provedor de serviços pode armazenar os dados do cliente, mesmo que temporariamente. - Definir as responsabilidades em caso de vazamento de informações.	**Política de Segurança da Informação** Deve conter, mas não se limitar à: - Esclarecer os requisitos de segurança de informações aplicáveis ao projeto e implementação do serviço em nuvem; - Informar os riscos de pessoas autorizadas em ambiente híbrido; - Informar a aplicabilidade ou não do acesso aos ativos de clientes pela equipe do provedor; - Estabelecer procedimentos de controle de acesso, incluindo autenticação multi-fator para acesso administrativo a serviços em nuvem; - Descrever sobre segurança de virtualização; - Estabelecer diretrizes de acesso e proteção dos dados do cliente; - Gerenciar o ciclo de vida de contas de clientes;

Cliente de Serviço em Nuvem	Provedor de Serviço em Nuvem
Programas de conscientização e treinamento: Deve conter, mas não se limitar à: - Normas e procedimentos para o uso de serviços em nuvem; - Gerenciamento dos Riscos de segurança da informação; - Considerações legais e regulamentares aplicáveis.	**Programas de conscientização e treinamento**: Deve conter, mas não se limitar à: - Fornecer conscientização e treinamento para os funcionários e garantir que os terceiros façam o mesmo, com relação ao tratamento adequado dos dados do cliente e dos dados derivados do serviço de nuvem.
Inventário de Ativos Deve conter, mas não se limitar à: - Contabilizar o inventário de ativos do cliente, as informações e os ativos associados armazenados no ambiente em nuvem. Os registros do inventário devem indicar onde os ativos são mantidos, por exemplo, identificação do serviço.	**Inventário de Ativos** Deve conter, mas não se limitar à: - O inventário de ativos do provedor deve identificar dados do cliente; - Assegurar que o inventário de ativos seja devidamente gerenciado.
Controle de Acesso Deve conter, mas não se limitar à: - Informar os requisitos de autenticação secreta, como senhas ao provedor. - Garantir que o acesso às informações no serviço de nuvem possa ser restrito de acordo com sua política de controle de acesso e que tais restrições sejam realizadas. - Não deve permitir que o gerenciamento das senhas de acesso seja realizado pelo provedor. - Estabelecer e aplicar as políticas de segurança para controle de acessos.	**Controle de Acesso** Deve conter, mas não se limitar à: - Fornecer informações sobre procedimentos para o gerenciamento de autenticação secreta do cliente, incluindo os procedimentos para alocação de tais informações e para autenticação do usuário. - Fornecer controles de acesso que permitam ao cliente restringir o acesso a seus serviços de nuvem, suas funções de serviço de nuvem e os dados do cliente mantidos no serviço.

Cliente de Serviço em Nuvem	Provedor de Serviço em Nuvem
Criptografia de Dados Deve conter, mas não se limitar à: - Revisar todas as informações fornecidas pelo provedor para confirmar a capacidade de criptografia. - Verificar a aplicação da criptografia dos dados em repouso e em trânsito (em uso).	**Criptografia de Dados** Deve conter, mas não se limitar à: - Fornecer informações ao cliente em relação às circunstâncias nas quais usa criptografia para proteger as informações que processa. - Fornecer informações ao cliente sobre quaisquer recursos que possam ajudá-lo a aplicar sua própria proteção criptográfica.
Gerenciamento de Mudanças Deve conter, mas não se limitar à: - Avaliação de impacto das mudanças executadas pelo provedor (vide capítulo 'Gerenciamento de Mudanças').	**Gerenciamento de Mudanças** Deve conter, mas não se limitar à: - Estabelecer formalmente a necessidade de comunicação ao cliente sobre alterações que possam afetar adversamente o serviço de nuvem. - Realizar a notificação do início e conclusão das alterações ao cliente.
Backup* e *Restore Deve conter, mas não se limitar à: - Solicitar as especificações do recurso de *backup* do provedor. - Ser responsável pela implementação de recursos de *backup* e restore quando o provedor de serviços em nuvem não os fornece ou por opção do cliente. - Verificar, quando responsabilidade de realização do *backup* pelo cliente, a sua execução, bem como cronograma de realização deste período de retenção dos dados, testes de *restore* e local de armazenamento. Esses processos devem ser gerenciados através de procedimentos.	***Backup* e *Restore*** Deve conter, mas não se limitar à: - Fornecer as especificações de seus recursos de *backup* e *restore* para o cliente. As especificações devem incluir as seguintes informações, conforme apropriado: - Escopo e cronograma de *backups*; - Métodos de *backup* e formatos de dados, incluindo criptografia, se relevante; - Períodos de retenção para dados de *backup*; - Procedimentos para verificar a integridade dos dados de backup e *restore*; - Procedimentos e cronogramas envolvidos na restauração de dados de *backup*; - Procedimentos para testar os recursos de *backup* e *restore*; - Local de armazenamento dos *backups*. - Fornecer acesso seguro e separado a *backups*, como imagens das máquinas virtuais, se aplicável.

Cliente de Serviço em Nuvem	Provedor de Serviço em Nuvem
Plano de Contingência Deve conter, mas não se limitar à: - Definir a estratégia de comunicação às áreas impactadas. - Definir as diretrizes do plano de contigência em conjunto com o provedor quando aplicável, bem como seu fluxo de atuação. - Definir as estratégias de plano de contingência interno até o plano de contingência do provedor ser estabelecido.	**Plano de Contingência** Deve conter, mas não se limitar à: - Comunicar as áreas impactadas e atuar conforme a definição do plano estabelecido para o cliente. - Definir o tempo-resposta para implementação do plano de contingência.
Sincronização de horário Deve conter, mas não se limitar à: - Solicitar informações sobre a sincronização do relógio usada para os sistemas do provedor de serviços em nuvem.	**Sincronização de horário** Deve conter, mas não se limitar à: - Fornecer informações ao cliente com relação ao relógio usado pelos sistemas do provedor e informações sobre como o cliente pode sincronizar os relógios locais com o relógio do serviço em nuvem.
Segregação de rede Deve conter, mas não se limitar à: - Definir requisitos para segregação de redes em ambiente compartilhado de um serviço de infraestrutura em nuvem.	**Segregação de rede** Deve conter, mas não se limitar à: - Provisionar a segregação de acesso à rede, quando aplicável.
Gerenciamento de incidentes Deve conter, mas não se limitar à: - Assegurar a conformidade do processo de gerenciamento de incidentes do provedor. - Realizar o gerenciamento, através de procedimentos, as ações corretivas e preventivas aplicáveis. - Fornecer, quando aplicável, comunicação formal dos dados do incidente interno que tenha relação com o serviço contratado.	**Gerenciamento de incidentes** Deve conter, mas não se limitar à: Fornecer ao cliente a documentação que abrange: - o escopo de incidentes de segurança da informação que o provedor relatará ao cliente; - o nível de divulgação da detecção de incidentes de segurança da informação e as respostas associadas ao cliente; - o prazo em que as notificações de incidentes de segurança da informação ocorrerão; - informações de contato para o tratamento de problemas relacionados a incidentes de segurança da informação; - quaisquer ações corretivas e preventivas que possam ser aplicadas.

11.1. Contrato de Aplicações em Nuvem

Ao decidir contratar uma aplicação em nuvem, deve ser considerado a elaboração do contrato de nível de serviço (SLA), com intuito de delinear as responsabilidades e processos a serem assistidos por ambas as partes, atribuindo peso legal ao contrato.

Este documento deve conter uma breve introdução e escopo do serviço a ser contratado e deve ser elaborado, antes da contratação formal dele. Como pré-requisito para elaboração do acordo, é premissa que tenha sido efetuado a qualificação do fornecedor e delineado os parâmetros de tempo de resposta para solução de incidentes para que posteriormente possa ser definido o monitoramento de desempenho do serviço prestado.

É de suma importância quando tratar-se de contratação de *IaaS* e *SaaS* avaliar se o provedor possui certificações, como por exemplo, ISO 27001, GDPR, HIPAA, SOC. Essas certificações visam demonstrar que o provedor possui conformidade internacional mantida por auditoria regular, assegurando assim as políticas de segurança de dados.

Há situações em que o provedor estabelece um SLA interno, e cabe ao cliente aceitá-lo e verificar a necessidade de implementação de processos adicionais internos.

O SLA e/ou contrato de serviços em nuvem deve conter, mas não se limitar à:

- Responsabilidade entre as partes;
- Confidencialidade dos dados;
- Monitoramento de desempenho;
- Gerenciamento de incidentes;
- Gerenciamento de mudanças;
- Gerenciamento das permissões de acesso;
- *Backup* e restauração;
- Recuperação de Desastre;
- Portabilidade.

Observação: Caso o SLA não trate de todos os itens supracitados, poderá ser realizada a coleta de documentos e evidências de igual valor que atendam esses itens.

O provedor de serviços em nuvem deve fornecer as informações e o suporte técnico necessário para atender aos requisitos de segurança de informação do cliente. Quando os controles de segurança da informação fornecidos pelo provedor são predefinidos e não podem ser alterados pelo cliente, esse pode precisar implementar controles adicionais para mitigar os riscos.

A responsabilidade do gerenciamento dos riscos referente à contratação de serviços em nuvem é do cliente, no entanto, o controle desses deve ser compartilhado entre o cliente e o provedor, como elucidado na tabela a seguir:

	Nuvem Privada (auto hospedado)	Nuvem Privada (co-localizado)	Infraestrutura como serviço (IaaS)	Plataforma como serviço (PaaS)	Software como serviço (SaaS)
Segurança de Governança, Risco e Conformidade (GRC)					
Segurança de Dados					
Segurança de Aplicações					
Segurança de Plataforma					
Segurança de Infraestrutura					
Segurança Física					

Legenda	
	Responsabilidade da Empresa Contratante
	Responsabilidade da Contratada e do Contratante
	Responsabilidade da Contratada (Provedor de Nuvem)

Figura 3 - Responsabilidades Contratada e Contratante

11.2. Confidencialidade dos Dados

A confidencialidade dos dados também deverá ser pautada no SLA. O acordo de confidencialidade, também chamado de NDA (do inglês "*Non Disclosure Agreement*") se trata de um documento com valor jurídico que pode ser utilizado por duas ou mais partes quando pretende-se manter informações em sigilo, evitando problemas como a espionagem industrial e o vazamento de dados corporativos.

O SLA deverá ser elaborado por equipe multidisciplinar, incluindo as áreas de tecnologia da informação, jurídico e qualidade (não limitadas às áreas citadas). Esse poderá prever penalidades, caso haja o descumprimento de algum dos itens estabelecidos; podendo ser realizado através do pagamento de multas ou de apuração de possíveis prejuízos, conforme definido em contrato.

O SLA aplica-se usualmente para contratação de *SaaS,* mas para os casos de contratação de *IaaS* é comumente utilizado o contrato virtual.

É importante salientar que o SLA deve detalhar, de maneira clara e objetiva, quais informações devem ser protegidas e de quem é a responsabilidade no caso de vazamento de informações.

11.3. Gerenciamento de Incidentes

É o processo responsável por gerenciar o ciclo de vida de todos os incidentes. O objetivo essencial do Gerenciamento de Incidentes é o retorno pelo provedor de serviços responsável ao cliente, o mais rápido possível.

Todos os eventos inesperados reportados para o provedor de serviço devem ser gerenciados por um sistema de Gerenciamento de Incidentes, com o objetivo de estruturar e documentar um relatório do ciclo de vida de incidentes, com investigação, diagnóstico, solução, prazo, conclusão, bem como ações preventivas e corretivas, a fim de evitar reincidência.

Um relatório de gerenciamento de incidentes poderá ser fornecido ao contratante em períodos regulares para permitir o gerenciamento e monitoramento de desempenho da aplicação (que pode ser uma tarefa compartilhada) e serviços em nuvem.

Se um incidente tem impacto na disponibilidade de dados ou integridade e/ou funcionalidade da aplicação, o incidente deve ser sistematicamente tratado como um problema no qual deve ser identificada a causa raiz para serem prevenidas recorrências, responsabilidade da parte que for responsável pelo incidente.

11.4. Monitoramento de Desempenho

O Monitoramento de Desempenho é o processo responsável pelas atividades diárias de gerenciamento de capacidade do serviço. Isso inclui monitoramento e análise através de indicadores estabelecidos no SLA, que podem ser preferencialmente embasados na definição SMART (*Specific, Measurable, Achievable, Relevant and Time based* - Específico, Mensurável, Alcançavel, Relevante e Temporal).

Alguns exemplos de indicadores que podem ser utilizados para monitoramento do desempenho de serviço são:

- Disponibilidade do serviço;
- Tempo limite para atendimento;
- Tempo de resposta ao incidente;
- Período médio entre falhas.

Deverão ser estabelecidas métricas e padrões para a medição de desempenho e da eficácia da gestão de segurança da informação. As organizações devem, no mínimo, compreender e documentar as métricas atuais e como elas mudarão quando as operações forem movidas para um serviço de computação em nuvem, que pode ser um provedor onde as métricas usadas sejam diferentes (potencialmente incompatíveis).

11.5. Gerenciamento de Mudanças

É o processo responsável por controlar o ciclo de vida de todas as mudanças na aplicação. O objetivo principal do gerenciamento de mudanças é permitir que melhorias sejam realizadas, com o mínimo de interrupção nos serviços de TI, mantendo a conformidade regulatória. Durante o gerenciamento de mudanças, o impacto da mudança no estado "validado" do sistema deve ser avaliado, para que seja mantido. Deste modo, é necessário realizar uma avaliação de impacto,

para determinar as atividades a serem realizadas, a fim de manter o estado validado do sistema. A responsabilidade pelo processo de Gerenciamento de Mudanças é compartilhada (contratante/contratada).

A contratada não poderá realizar mudanças sem o prévio conhecimento da contratante, um exemplo das etapas envolvidas no fluxo de mudanças está descrito na tabela abaixo:

Etapa	**Atividades**
Início do processo de controle de mudanças	Um formulário de Solicitação de Mudança é feito pelo Solicitante (podendo ser tanto pelo contratante quanto pelo contratado) para incluir uma descrição detalhada da alteração solicitada, a justificativa para a mudança, o impacto potencial, se conhecido, e a prioridade.
Avaliação do impacto da mudança	Avaliação do impacto da mudança, por equipe multidisciplinar e definição dos esforços necessários. Recomenda-se elaborar Análise de Riscos para avaliação. A primeira avaliação da prioridade e necessidade de mudança é feita. Se a requisição de mudança for negada, o solicitante deve ser informado.
Aprovação da solicitação de mudança	Quando a avaliação está completa, a solicitação de mudança é aprovada. Solicitações de mudança BPx relevantes (impacto em boas práticas) devem ser encaminhadas para aprovação da Unidade de Qualidade.
Implementação da mudança	A implementação da mudança inclui todas as atividades descritas no Ciclo de Vida do Sistema, de acordo com o tipo, conforme elucidado na figura 4.
Liberação para produção	O pré-requisito para esta etapa é a conclusão das atividades relacionadas ao ciclo de vida do sistema descritas na ferramenta de controle de mudanças.
Encerramento da Mudança	Uma solicitação de mudança deve ser fechada quando as atividades descritas nas etapas anteriores estiverem completas e as partes responsáveis aprovarem.

A avaliação de risco deve considerar o impacto potencial sobre: o sistema, o produto e usuários finais, além de empregar uma abordagem multifacetada para o controle. O processo abrangente deve permitir escalabilidade na maioria dos sistemas BPx. A metodologia proposta para análise de risco tem como meta quatro (4) categorias de avaliação de risco: definir, identificar, interpretar / quantificar e aplicar. Empregando a metodologia proposta, permitirá uma compreensão dos riscos potenciais associados às alterações na configuração BPx, e estabelecimento de um catálogo de mudanças no sistema com níveis variáveis de controle baseado em risco.

A figura 4 apresenta uma visão geral da abordagem proposta baseada no risco com base nesta metodologia.

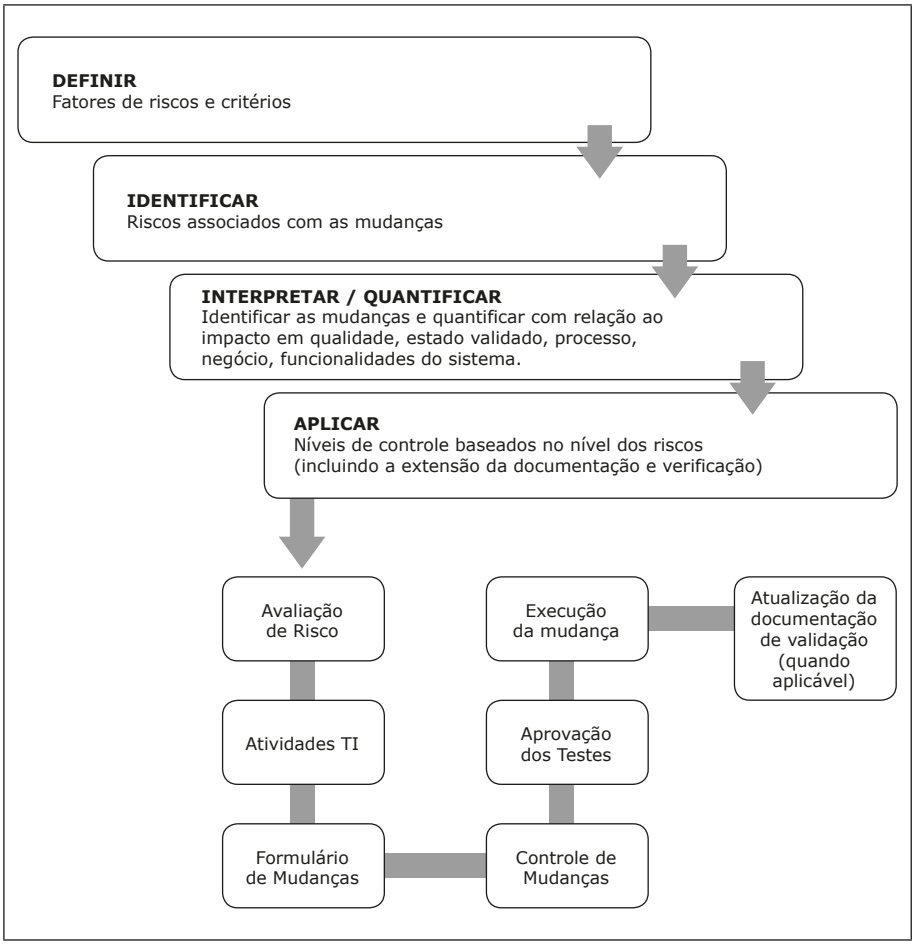

Figura 4 - Diagrama da Abordagem Baseada no Risco ou Processo de Risco Proposto

Etapa 1: Definir risco

A definição de risco é essencial para a aplicação de um programa de gerenciamento de qualidade e é um passo crucial antes do início da análise de mudança específica. O GAMP 5 declara: "A gestão do risco de qualidade deve basear-se em compreensão do processo e impacto potencial na segurança do paciente, na qualidade do produto e na integridade dos dados".

Para fins deste documento, o escopo da qualidade do produto refere-se à saída controlada do sistema, ou mais especificamente para a qualidade / integridade do conteúdo de estado final.

Etapa 2: Identificação do(s) Risco(s)

O GAMP 5 afirma que "a aplicação do gerenciamento de risco de qualidade permite que o esforço seja focado em aspectos críticos de um sistema computadorizado de maneira controlada e justificada". Para alcançar esse objetivo, a identificação do risco engloba uma visão minusciosa de todas as possíveis mudanças e a validação completa dessas possíveis mudanças com base nas definições de riscos estabelecidos. Quanto mais abrangente for a abordagem empregada para essa etapa, maior será a consistência e os benefícios realizados para a aplicação contínua do controle baseado em risco.

Etapa 3: Interpretação/quantificação dos riscos

Depois que os riscos são adequadamente definidos e identificados, eles devem ser traduzidos em categorias facilmente entendidas, que facilitam a aplicação baseada em riscos. No que diz respeito à interpretação dos riscos, o ICH Q9 afirma que a avaliação do risco de qualidade deve basear-se no conhecimento científico e, em última instância, vincular-se à proteção do paciente e à integridade do conteúdo de estado final controlado (*software*).

A quantificação deve ser feita por pessoal treinado que compreenda os aspectos gerenciais do sistema. Incluindo, entre outros, ciclos de vida, fluxos de trabalho, configurações de segurança, registros eletrônicos, operações do sistema e análise de dados.

Etapa 4: Aplicar um nível adequado de controle de risco

O nível de controle não deve comprometer a visibilidade do risco inerente, ou a qualidade/conformidade do sistema. Embora a manutenção da qualidade seja primordial, a abordagem aplicada deve ser escalável e facilitar a comunicação pró-ativa e em tempo real para o gerenciamento de mudanças na configuração. O conceito de risco aplicado do ICH Q9 declara que "o nível de esforço, formalidade e documentação do processo de gestão do risco da qualidade ser proporcional ao nível de risco". Deve-se aplicar este conceito para o gerenciamento de mudanças na configuração BPx, gestão, confirmação e qualificação baseado no risco potencial da mudança para o sistema e o resultado do sistema.

11.6. Gerenciamento das Permissões de Acesso

O gerenciamento das permissões de acesso à nuvem também deve ser tratado no contrato. É importante delinear quem será o responsável por essa atividade, além de descrever que as senhas deverão ser individuais, criptografadas, com periodicidade de expiração, políticas de senhas fortes (caracteres especiais, letras, números, maiúsculo, minúsculo), assegurar que não tenha usuário genérico, dentre outros.

Pode ser solicitado ao fornecedor da nuvem que o controle de acesso seja realizado para cada usuário, através de perfis de acesso, contendo informações de quem pode criar, excluir, visualizar, exibir *logs* de acesso e escolher a região geográfica onde serão armazenados os perfis de acesso e seu conteúdo (por regulamentação local, por exemplo).

11.7. *Backup* e Restauração dos Dados e da Aplicação

Os dados armazenados no sistema precisam ser legíveis e recuperáveis durante todo o período de retenção do registro associado, assim como a aplicação precisa ser mantida adequadamente para garantir que os registros arquivados sejam prontamente recuperáveis e legíveis.

Deverá ser definido no SLA o tempo de resposta esperado entre a abertura do chamado para realização do processo de backup e/ou restauração, levando em consideração a criticidade do incidente aberto. Para mais informações, consultar capítulo '*Backup* e Recovery na Nuvem'.

11.8. Recuperação de Desastre

O SLA deverá conter políticas e procedimentos relacionados à preparação para o retorno ao funcionamento do sistema por perda completa de um ou mais componentes importantes, denominado Recuperação de Desastre (*Disaster Recovery*). O SLA poderá mencionar uma política de recuperação de desastre, abrangendo ações a serem adotadas antes, durante e após um desastre.

Deverá ser descrito detalhes minuciosos da estrutura existente, componentes envolvidos no negócio, pessoal responsável por realizar a recuperação, métodos de comunicação no momento do desastre, instalação alternativa para a organização, quando aplicável.

11.9. Plano de Continuidade do Negócio

O planejamento de continuidade de negócios inclui o planejamento de contingência sobre como o negócio operará em caso de indisponibilidade do serviço.

No SLA devem ser definidos, mas não se limitando à:

- Responsáveis impactados que devem ser comunicados;
- Por quanto tempo o sistema pode ficar indisponível antes da aplicação da estratégia;
- O processo de negócios a ser seguido até que o sistema esteja disponível novamente.

11.10. Portabilidade

A portabilidade é o processo de mover dados/serviços de um provedor para outro, ou levá-lo totalmente de volta para a empresa. A habilidade de portabilidade e interoperabilidade deve ser considerada desde o início do projeto como parte do gerenciamento de risco e da garantia da segurança de quaisquer programas de contratação em nuvem, através do SLA.

Os SLAs podem ser diferentes entre provedores e, é preciso compreender como isso pode afetar a sua capacidade de trocar de provedor.

Os sistemas na nuvem podem residir em arquiteturas de plataformas diferentes. É importante estar ciente de como elas limitarão a portabilidade através

da compreensão das dependências de serviço de plataforma, que podem incluir *APIs*, *hypervisors*, a lógica de aplicações e demais restrições (*lock in*, termo utilizado para definir grau de dificuldade de deixar o vendor contratado).

Todos os itens mencionados neste Guia como recomendados para serem citados em contratos poderão ser encontrados em outros documentos formais de mesma relevância que o SLA ou contrato.

Conclusões

12. Conclusões

Diante da realidade da implementação do uso de serviços em ambiente de cloud pelas empresas do segmento de ciências da vida, tem-se a importância das implicações em termos de qualidade a que este guia se propôs em discutir e trazer a aplicação das boas práticas a serem adotadas para as soluções em nuvem. Trata-se de um segmento em contínua expansão e adaptação aos quesitos de BPx, que por conta do desenvolvimento de novas tecnologias passará por novos aprimoramentos que torna a discussão deste tema constante, uma vez que novas regras e soluções integrarão os temas abordados neste guia.

A regulamentação geralmente vem depois das tecnologias que normalmente trazem possibilidades de melhor desempenho e controle aos processos. Contudo, devemos estar abertos a elas desde que adotadas as boas práticas baseadas em riscos.

As agências reguladoras têm o papel de controle sanitário dos produtos acabados das empresas. Quem deve aceitar ou não os riscos das novas tecnologias são os regulados, o que é totalmente possível quando adotadas as boas práticas baseadas em riscos. Os órgãos reguladores desejam verificar a conformidade, conhecimento e controle dos processos do regulado e seus respectivos riscos.

Como a tecnologia evolui constantemente, é de suma importância o monitoramento das legislações e regulamentações que apoiam tais implementações.

Esperamos que o conteúdo deste material possa auxiliar na estruturação deste assunto tão vasto e importante ao segmento e que as empresas compreendam que é possível (ou até mais seguro) trabalhar com os sistemas e dados em nuvem desde que adotadas as boas práticas abordadas neste guia.

Referências

13. Referências

O grupo de trabalho utilizou as seguintes referências:

1. Amazon Web Services, Inc.
2. Microsoft Azzure.
3. Google Cloud Plataform
4. CSA – Security Guidance: Guia de segurança em computação em nuvem. CSA - Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing v4.0, publicado em 2017.
5. ENISA – Cloud Computing: ENISA (European Network and Information Security Agency) - Cloud Computing Benefits, risks and recommendations for information security, publicado em dezembro de 2012.
6. GAMP5 - Good Automated Manufacturing Practices - Versão 5 – Guia Internacional de Validação de Sistemas.
7. Guia de Validação de Sistemas Computadorizados ANVISA/2010.
8. ICHQ9 - International Conference on Harmonization of Technical Requirements for Registration of Pharmaceuticals for Human Use - Quality Risk Management Q9 – 2005.
9. ISO / IEC 27017: Norma de segurança para serviços em nuvem. ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission): Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services, publicada em julho de 2015.
10. NIST - National Institute of Standards and Technology - Cloud Computing Synopsis and Recommendations, publicado em maio de 2012. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf.
11. https://docplayer.net/1998659-Oracle-database-backup-in-the-cloud-an--oracle-white-paper-september-2008.html.
12. Guia ISPE Qualificação de Infraestrutura, segunda edição.
13. ISO/IEC 27000: (in force), Information technology – Security techniques – Information security management systems – Overview and vocabulary.
14. ISO 27001: Information technology - Security techniques - Information security management systems – Requirements.
15. ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls.
16. ISO/IEC 27007: Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
17. ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.
18. NIST Special Publication 800-190: Application Container Security Guide.

ISBN 978-85-60162-73-4

SINDUSFARMA