# Acórdão TCU 1.793/2015-Plenário

# Anexo I - Tabela de riscos, controles possíveis e critérios

|  |  |
| --- | --- |
| **Tema:  Segurança da informação** | |
| **Categoria de risco: Indisponibilidade do serviço** | |
| **Risco específico** | |
| 1- Não implementação de controles e salvaguardas suficientes para garantir a continuidade da infraestrutura do provedor, afetando assim a disponibilidade do serviço para o usuário final | |
| **Controles possíveis** | **Critérios** |
| O plano de continuidade de negócio deve considerar as partes do negócio que estão na nuvem e levar em consideração tanto as características do negócio como do provedor | COBIT DSS04 - Manage Continuity |
| Considerar capacidade do provedor de trabalhar com multirregiões no provedor e poder transferir carga de uma região para outra |
| O plano de continuidade de negócio para nuvem pode considerar mais de um provedor como contingência |
| Considerar a alternativa de utilizar sua própria infraestrutura de TI como contingência |
| OS SLAs com o provedor de nuvem devem ser cuidadosamente definidos e exequíveis, o que inclui penalidades em caso de não cumprimento | COBIT APO10 - Manage Suppliers ; COBIT APO09 - Manage Service Agreements |
| **Risco específico** | |
| 2 - Indisponibilidade de elementos da infraestrutura do cliente que são críticos para o acesso a serviços na nuvem | |
| **Controles possíveis** | **Critérios** |
| Deve ser definido e documentado um método para determinar o impacto de qualquer indisponibilidade à organização, incluindo de serviços que estão na nuvem, que deverá, também, estabelecer prioridades para recuperação e período máximo tolerável para a indisponibilidade | COBIT DSS04 - Manage Continuity; CSA CCM BCR-09 |
| **Categoria de risco: Confidencialidade e integridade de dados** | |
| **Risco específico** | |
| 3 - Controle de acesso inexistente ou insuficiente para assegurar a confidencialidade dos dados armazenados na nuvem | |
| **Controles possíveis** | **Critérios** |
| Os dados devem ser submetidos à classificação prévia da informação, antes de serem transmitidos para a nuvem | COBIT APO13 - Manage Security; COBIT BAI09 - Manage Assets; CSA CCM DSI-01 |
| Implementar controle de acesso lógico apropriado ao grau de confidencialidade dos dados armazenados na nuvem | COBIT DSS05 - Manage Security Services; CSA CCM IAM-02 e IAM-05 |
| **Risco específico** | |
| 4 - A segurança dos dados transmitidos para o provedor de nuvem pela internet pode ser comprometida durante a transferência | |
| **Controles possíveis** | **Critérios** |
| Implementar controles para transferência de dados, como criptografia e uso de VPN adequada | COBIT DSS05 - Manage Security Services; CSA CCM DSI-01 |
| **Risco específico** | |
| 5 - Acesso indevido do provedor aos dados | |
| **Controles possíveis** | **Critérios** |
| Estabelecer políticas e procedimentos para o uso de criptografia, incluindo gerenciamento de chaves criptográficas, que devem ser seguidos pelo cliente e pelo provedor | COBIT DSS05 - Manage Security Services; CSA CCM EKM-02, EKM-03 e EKM-04 |
| As chaves criptográficas não devem ser armazenadas na nuvem |
| Os dados armazenados no provedor devem estar criptografados, sendo que o esquema criptográfico deve ser adequado à classificação das informações |
| Definir cláusulas contratuais estabelecendo limites do acesso do provedor aos dados do cliente | COBIT APO09 - Manage Service Agreements; COBIT APO10 - Manage Suppliers |
| **Risco específico** | |
| 6 - O provedor pode ser forçado legalmente a fornecer dados por estar submetido a jurisdição estrangeira, colocando em risco a privacidade e a disponibilidade das informações | |
| **Controles possíveis** | **Critérios** |
| Os dados armazenados no provedor devem estar criptografados | COBIT DSS05 - Manage Security Services; CSA CCM EKM-03 e DSI-02 |
| O provedor deve assegurar que dados sujeitos a limites geográficos não sejam migrados para além de fronteiras definidas em contrato |
| **Risco específico** | |
| 7 - Um cliente pode ter acesso indevido a dados de outro cliente | |
| **Controles possíveis** | **Critérios** |
| O provedor deve garantir e demonstrar isolamento de recursos e de dados de seus clientes | COBIT DSS05 - Manage Security Services |
| Definir cláusulas contratuais estabelecendo responsabilidade do provedor em garantir o isolamento de recursos e dados contra acesso indevido por outros clientes | COBIT APO09 - Manage Service Agreements; COBIT APO10 - Manage Suppliers |
| **Risco específico** | |
| 8 - Acesso indevido à medida que os serviços de computação em nuvem são amplamente acessíveis, independentemente de localização | |
| **Controles possíveis** | **Critérios** |
| O provedor deve garantir controles eficazes e compatíveis com as políticas e procedimentos do cliente para gerenciamento de identidades de usuários e controle de acessos | COBIT DSS05 - Manage Security Services |
| **Categoria de risco: Gestão de mudanças** | |
| **Risco específico** | |
| 9 - A gestão de mudanças do provedor de computação em nuvem pode não ser adequada às necessidades do cliente. Por exemplo, mudanças na infraestrutura de software do provedor (patch corretivo, atualização de versão etc) podem não passar por processos de gestão de mudanças individuais dos clientes, causando impactos negativos (risco agravado em caso de SaaS) | |
| **Controles possíveis** | **Critérios** |
| A política para gestão de mudanças deve ser acordada entre provedor e cliente, e este último deve ser comunicado com antecedência sobre mudanças (por exemplo, utilizando processos do ITIL) | COBIT BAI06 - Manage Changes; CSA CCM CCC-02 |
| **Categoria de risco: Trilhas de auditoria** | |
| **Risco específico** | |
| 10 - A política do provedor para liberar os logs de acesso, de sistema e de segurança não atende aos requisitos do cliente; há perda ou fornecimento incompleto de informações do provedor para o cliente relativas a incidentes de segurança e ao fornecimento de trilhas de auditoria | |
| **Controles possíveis** | **Critérios** |
| Cláusulas contratuais devem definir políticas e procedimentos que devem ser estabelecidos para triagem dos eventos relacionados à segurança e garantir o gerenciamento de incidentes completo e ágil | COBIT DSS02 - Manage Service Requests and Incidents; COBIT DSS05 - Manage Security Services; COBIT APO10 - Manage Suppliers; CSA CCM SEF-02 e SEF-03 |
| Eventos de segurança de informação devem ser comunicados através de canais predefinidos de comunicação, de maneira rápida e eficiente, e de acordo com os requisitos legais, regulatórios e contratuais |
| Logs de auditoria do provedor que registram atividades de acesso de usuários privilegiados, tentativas de acesso autorizados e não autorizados, exceções do sistema, e eventos de segurança da informação devem ser mantidos em conformidade com as políticas e regulamentos aplicáveis, e devem estar de acordo com as políticas do cliente |
| **Risco específico** | |
| 11 - Logs possuem período de retenção no provedor menor que o esperado e estabelecido nas políticas internas do cliente | |
| **Controles possíveis** | **Critérios** |
| O cliente deve prever cópia dos logs fornecidos pelo provedor, de acordo com sua própria política de retenção; deve haver, da parte do provedor, um mecanismo para filtragem e cópia dos logs gerados pelo fornecedor para a área do cliente | COBIT DSS05 - Manage Security Services |
| **Risco específico** | |
| 12 - Ausência de isolamento de logs entre vários clientes; vazamento de dados de log | |
| **Controles possíveis** | **Critérios** |
| O contrato entre cliente e provedor deve estabelecer direitos claros e exclusivos de propriedade e acesso aos dados, inclusive referentes a logs | CSA CCM IAM-01 |
| O acesso e uso de ferramentas de auditoria que interajam com os sistemas de informação das organizações deverão estar devidamente segmentados e restritos para evitar comprometimentos e uso indevido de dados de log |
| **Categoria de risco: Segurança de interfaces de programação (APIs)** | |
| **Risco específico** | |
| 13 - As APIs para acesso à infraestrutura do provedor e aos dados do cliente possuem falhas ou vulnerabilidades | |
| **Controles possíveis** | **Critérios** |
| O modelo de segurança das interfaces do provedor deve ser desenvolvido com base em padrões de mercado, incluindo mecanismos de autenticação forte de usuários e controle de acesso para restringir o acesso aos dados do cliente | CSA CCM AIS-01, AIS-02, AIS-03 e AIS-04 |
| **Categoria de risco: Acesso indevido por invasor interno** | |
| **Risco específico** | |
| 14 - As políticas e orientações do provedor de nuvem quanto ao acesso de seus funcionários aos ativos físicos e virtuais podem não ser adequadas ou de conhecimento do cliente | |
| **Controles possíveis** | **Critérios** |
| Definir no contrato as obrigações do provedor quanto a requisitos mínimos de autorização e transparência de acesso do provedor aos ativos físicos e virtuais do cliente, bem como a respeito da necessidade de divulgação ao cliente de suas políticas e orientações específicas | COBIT APO10 - Manage Suppliers; CSA CCM HRS-06, HRS-07, IAM-02, IAM-04, IAM-07 e IAM-09 |
| **Risco específico** | |
| 15 - As políticas e orientações do provedor quanto a contratação de pessoal, monitoramento de atividades de seus funcionários e verificação do cumprimento das normas organizacionais podem não ser adequadas ou de conhecimento do cliente | |
| **Controles possíveis** | **Critérios** |
| Definir no contrato as obrigações do provedor quanto a requisitos mínimos de contratação de pessoal e de monitoramento de suas atividades, bem como a respeito da necessidade de divulgação ao cliente de suas políticas e orientações específicas | COBIT APO10 - Manage Suppliers; CSA CCM HRS-02, HRS-03, HRS-06, HRS-07, HRS-09, IAM-07 e IAM-10 |
| **Categoria de risco: Atualizações e correções de segurança** | |
| **Risco específico** | |
| 16 - Exploração de vulnerabilidades do provedor podem impactar operações do cliente | |
| **Controles possíveis** | **Critérios** |
| Políticas, procedimentos e mecanismos devem ser estabelecidos e implementados pelo provedor para gerenciamento de vulnerabilidades conhecidas e atualizações de software, garantindo que aplicações, sistemas e vulnerabilidades de dispositivos de rede sejam avaliadas, e que atualizações de segurança fornecidas sejam aplicadas em tempo hábil, priorizando os patches mais críticos | COBIT DSS05 - Manage Security Services; CSA CCM TVM-01 e TVM-02 |
|  |  |
| **Tema:  Governança e gestão de riscos** | |
| **Categoria de risco: Planejamento** | |
| **Risco específico** | |
| 17 - Dimensionamento inadequado das vantagens e riscos relativos à incorporação de serviços de computação em nuvem em função das características e requisitos individuais da organização | |
| **Controles possíveis** | **Critérios** |
| A incorporação de computação em nuvem ao plano estratégico de TI deve ser precedida de análise adequada de modo a assegurar que serviços de nuvem são a solução mais apropriada para as necessidades da organização | COBIT APO02 - Manage Strategy ; COBIT APO08 - Manage Relationships |
| A incorporação de computação em nuvem ao plano estratégico de TI deve ser elaborada por um time de profissionais qualificados de TI e de negócio, e todas as partes interessadas na organização devem ser consultadas |
| **Risco específico** | |
| 18 - Planejamento orçamentário de TI não adequado às características de contratação de serviços de computação em nuvem | |
| **Controles possíveis** | **Critérios** |
| O planejamento orçamentário deve estar alinhado com as condições de contratação de serviços de computação em nuvem, particularmente quanto à transformação de verba de investimento na compra de equipamentos de TIC para verba de custeio dos serviços de nuvem | COBIT APO02 - Manage Strategy; COBIT APO04 - Manage Innovation; COBIT APO06 - Manage Budget and Costs |
| **Categoria de risco: Política de recursos humanos** | |
| **Riscos específicos** | |
| 19 - Resistência da equipe de TI à adoção de computação em nuvem por receio de perder suas funções | |
| **Controles possíveis** | **Critérios** |
| Deve ser conduzida política de recursos humanos de TI que contemple redefinições de funções e realocações de pessoal, considerando as capacidades e perfis individuais | COBIT APO07 - Manage Human Resources; COBIT APO08 - Manage Relationships; COBIT APO04 - Manage Innovation |
| Implementar política institucional de incentivo à inovação, como forma de estimular o servidor e quebrar resistência à adoção de computação em nuvem |
| **Categoria de risco: Governança** | |
| **Riscos específicos** | |
| 20 - Perda de governança e controle da TI por parte da organização quando da utilização de serviços na nuvem | |
| 21 - Menor reatividade do fornecedor a comandos do cliente se comparado a provimento interno do serviço | |
| **Controles possíveis** | **Critérios** |
| Definir cláusulas contratuais especificando nível esperado dos serviços (SLA) e mecanismos clássicos de gestão contratual de serviços terceirizados (comunicações formais, multas, rescisão etc) | COBIT APO10 - Manage Suppliers |
| Definir cláusulas contratuais especificando mecanismos de segurança e proteção de propriedade intelectual, e quaisquer requisitos legais ou regulatórios |
| Definir e formalizar, no contrato, papéis e responsabilidades do provedor de serviços de nuvem e do cliente |
| Estabelecer processos ágeis de contratação e migração para provedores alternativos, em caso de falhas do provedor principal |
| Definir em cláusula contratual a necessidade de realização de avaliações periódicas independentes, com a finalidade de verificar a adequação dos controles do provedor a um conjunto de critérios pré-definidos | CSA CCM AAC-01 e AAC-02 |
| **Risco específico** | |
| 22 - Falta de apoio interno devido à cultura organizacional e percepção do cliente de que há maiores riscos associados a serviços em nuvem | |
| **Controles possíveis** | **Critérios** |
| Promover política institucional de incentivo à inovação de maneira a convertê-la em parte da cultura organizacional | COBIT APO04 - Manage Innovation |
| **Categoria de risco: Legislação e normativos pertinentes** | |
| **Risco específico** | |
| 23 - Não observância de legislação e normativos específicos que regulam a contratação de serviços de computação em nuvem ou de pontos específicos em regulamentos de contratação de serviços de TI em geral | |
| **Controles possíveis** | **Critérios** |
| A organização deve ser capaz de assegurar a conformidade dos dados e aplicações hospedadas na nuvem com os requisitos de padrões, legais e regulatórios, aos quais o negócio está sujeito, de maneira contínua e atualizada | COBIT MEA03 - Ensure Compliance With External Requirements; CSA CCM AAC-03 |
| **Risco específico** | |
| 24 - Desconformidade com o Decreto 8.135/2013 e com a Portaria Interministerial 141/2014 | |
| **Controles possíveis** | **Critérios** |
| Verificar, na fase de planejamento da contratação, se o objeto da contratação pode ser enquadrado como "comunicação de dados da APF", conforme a Portaria Interministerial 141/2014, art. 1º e art. 11 | Decreto 8.135/2013; Portaria Interministerial 141/2014 |
| Até o término da fase de planejamento da contratação, verificar se a contratação deve ser feita por meio de provedor público ou privado, consultando a disponibilidade dos provedores públicos de atender às especificações técnicas e níveis de serviço do objeto da contratação, conforme a Portaria Interministerial 141/2014, art. 5º, § 3º |
| Especialmente no caso de contratação de fornecedor privado, observar os requisitos comuns de implementação dos serviços estabelecidos pela Portaria Interministerial 141/2014: padrões do e-Ping (art. 8º) e obrigações que deverão estar contidas no termo de referência ou projeto básico e no contrato (art. 9º) |
| Especialmente no caso de contratação de fornecedor privado, observar os requisitos específicos de implementação dos serviços estabelecidos pela Portaria Interministerial 141/2014: requisitos mínimos para serviços de redes de telecomunicações (art. 10) e critérios mínimos de segurança da informação (art. 12) |
| Especialmente no caso de contratação de fornecedor privado, observar os requisitos de auditoria de programas e equipamentos estabelecidos pela Portaria Interministerial 141/2014 (arts. 13 e 14), os quais deverão estar previstos no termo de referência ou projeto básico e no contrato |
| **Risco específico** | |
| 25 - Não observância das normas de segurança do DSIC/GSI/PR | |
| **Controles possíveis** | **Critérios** |
| No caso de infraestrutura de nuvem para sistemas estruturantes da APF, contratar órgão ou entidade da APF (item 4.2.3 da Norma Complementar 19/IN01/DSIC/GSIPR) | Norma Complementar 14/IN01/DSIC/GSIPR; Norma Complementar 19/IN01/DSIC/GSIPR |
| Antes de adotar a tecnologia de computação em nuvem, observar as diretrizes da sua Política de Segurança da Informação e Comunicações (SIC), do seu processo de Gestão de Riscos de SIC e do seu processo de Gestão de Continuidade de Negócios nos aspectos relacionados à SIC (item 5.1 da Norma Complementar 14/IN01/DSIC/GSIPR) |
| Ao contratar ou implementar um serviço de computação em nuvem, garantir que o ambiente, incluindo infraestrutura e canal de comunicação, esteja aderente às diretrizes e normas de SIC do GSI/PR, que a legislação brasileira prevaleça e que o contrato de prestação de serviço contenha cláusulas de segurança quanto às informações hospedadas na nuvem (item 5.2 da Norma Complementar 14/IN01/DSIC/GSIPR) |
| Avaliar quais informações serão hospedadas na nuvem, considerando o processo de classificação da informação, o valor do ativo de informação, os controles de acesso físicos e lógicos, o modelo de serviço e de implementação de computação em nuvem e a localização geográfica onde as informações serão armazenadas (item 5.3 da Norma Complementar 14/IN01/DSIC/GSIPR) |
|  |  |
| **Tema:  Contratação e gestão contratual** | |
| **Categoria de risco: Gestão contratual** | |
| **Risco específico** | |
| 26 - Níveis de serviço estabelecidos em contrato podem não ser cumpridos | |
| **Controles possíveis** | **Critérios** |
| Prever dispositivos contratuais que busquem assegurar os níveis de serviço no caso de interrupções de serviço planejadas ou não planejadas | COBIT APO9 - Manage Service Agreements |
| Definir em contrato modelo de remuneração vinculada aos níveis de serviço estabelecidos, prevendo glosas no caso de descumprimento de parâmetros mínimos |
| Definir em contrato sanções no caso de descumprimento reiterado de parâmetros mínimos de níveis de serviço estabelecidos |
| Prever soluções de contingência independentes de provedor específico (portabilidade do serviço para outro fornecedor, contrato de contingência em caso de falha do fornecedor principal, espelhamento do serviço em infraestrutura própria etc) |
| **Risco específico** | |
| 27 - Vulnerabilidades e problemas de segurança detectados no provedor demoram para ser corrigidos ou não são corrigidos | |
| **Controles possíveis** | **Critérios** |
| Assegurar que todas as vulnerabilidades sejam priorizadas e corrigidas dentro de SLAs acordados contratualmente entre cliente e provedor | COBIT APO9 - Manage Service Agreements; COBIT APO13 - Manage Security |
| O processo de gestão de vulnerabilidades do provedor deve ser transparente ao cliente |
| **Risco específico** | |
| 28 - Falhas no monitoramento e gestão contratuais | |
| **Controles possíveis** | **Critérios** |
| Definir no contrato uma divisão clara de papéis de cliente e provedor | COBIT APO10 - Manage Suppliers |
| Estabelecer no contrato indicadores claros e precisos tanto de ambiente como de segurança, com responsáveis pelo seu monitoramento e disponibilização |
| **Risco específico** | |
| 29 - Estouro de orçamento para o contrato devido à falta de controle sobre o uso dos recursos de computação em nuvem e estimativas imprecisas de custo | |
| **Controles possíveis** | **Critérios** |
| Prever verificações intermediárias do nível de uso da capacidade contratada, alertas quando atingidos patamares de recursos e tetos de recursos máximos utilizáveis em função do orçamento disponível | COBIT APO06 - Manage Budget and Costs |
| **Categoria de risco: Dependência frente ao provedor** | |
| **Riscos específicos** | |
| 30 - Dependência do cliente com relação ao provedor (vendor lock-in) | |
| 31 - Dificuldades do cliente em migrar dados de um provedor para outro ou internalizá-los novamente, por problemas de interoperabilidade ou de portabilidade | |
| 32 - A organização não previu e considerou custos de saída do provedor | |
| 33 - Indisponibilidade do fornecedor (ruptura contratual, falência, sequestro de dados) | |
| **Controles possíveis** | **Critérios** |
| Os requisitos da organização para portabilidade e interoperabilidade devem ser cuidadosamente avaliados antes da contratação de nuvem frente às alternativas disponíveis no mercado, a fim de mitigar relações de dependência com o provedor | COBIT BAI03 - Manage Solutions Identification and Build; CSA CCM IPY-01, IPY-02, IPY-03, IPY-04 e IPY-05 |
| Os provedores devem utilizar pacotes modulares, usar formatos abertos ou populares para dados e serviços, e serem transparentes em regulações e taxas aplicadas à transferência de dados |
| Processos, procedimentos e recursos devem ser estabelecidos e testados, de maneira a viabilizar a transferência de operações de um provedor de computação em nuvem para outro provedor alternativo |
| Especialmente no caso de informações críticas para o negócio, convém considerar a execução de plano de backup independente do fornecedor, duplicando dados em intervalos periódicos |
| Prever em contrato condições e limites claros de custos para saída do provedor |
| **Categoria de risco: Falhas contratuais** | |
| **Risco específico** | |
| 34 - Conflitos sobre a propriedade dos dados armazenados na nuvem | |
| **Controles possíveis** | **Critérios** |
| Incluir no contrato cláusula especificando que os direitos de propriedade sobre os dados armazenados na nuvem pela organização são exclusivos da organização | COBIT APO10 - Manage Suppliers; COBIT APO12 - Manage Risk; COBIT BAI03 - Manage Solutions Identification and Build |
| **Risco específico** | |
| 35 - Falta de delimitação legal regendo as relações contratuais, dado que os serviços de nuvem podem ser prestados globalmente | |
| **Controles possíveis** | **Critérios** |
| O contrato deve definir em quais países os dados do cliente podem ser armazenados | COBIT BAI03 - Manage Solutions Identification and Build |
| **Risco específico** | |
| 36 - Não exclusão de dados armazenados na nuvem ao término de um contrato | |
| **Controles possíveis** | **Critérios** |
| Deve ser previsto contratualmente que o provedor atenda à política de exclusão de dados do cliente | COBIT DSS05 - Manage Security Services |
| Utilizar criptografia para proteger os dados de acesso indevido |
| Utilizar técnicas de marca d'água para identificar origens de vazamento de informações sigilosas |
|  |  |
| **Tema:  Infraestrutura de TI** | |
| **Categoria de risco: Falhas relativas à infraestrutura de TI** | |
| **Riscos específicos** | |
| 37 - Falhas de isolamento entre ambientes ou instâncias virtuais de clientes diferentes | |
| 38 - O compartilhamento de recursos pelos provedores de nuvem entre vários clientes pode inserir vulnerabilidades adicionais | |
| **Controles possíveis** | **Critérios** |
| O provedor deve implementar controles para isolamento e segurança de sistema operacional | COBIT DSS05 - Manage Security Services; COBIT BAI010 - Manage Configuration; CSA CCM IVS-05, IVS-09 e IPY-05 |
| O provedor deve utilizar soluções de virtualização que sejam padrões ou referências de mercado |
| O provedor deve implementar política de atualização de versão de software e aplicação de correções |
| **Riscos específicos** | |
| 39 - As ferramentas e processos para gestão de incidentes do provedor podem ser incompatíveis com os utilizados pelo cliente | |
| 40 - O processo de gestão de incidentes do provedor apresenta falhas em documentação, resolução, escalonamento ou encerramento de incidentes | |
| **Controles possíveis** | **Critérios** |
| O contrato deve detalhar definições específicas de incidentes, eventos, ações a serem tomadas e responsabilidades do provedor e do cliente | COBIT APO09 - Manage Service Agreements; COBIT APO10 - Manage Suppliers; COBIT DSS02 - Manage Service Requests and Incidents; CSA CCM SEF-02, SEF-03 e STA-02 |
| O contrato deve definir requisitos de interoperabilidade entre as ferramentas de gestão de incidentes do provedor e do cliente |
| **Risco específico** | |
| 41 - Problemas de infraestrutura de rede do cliente podem afetar o desempenho dos serviços de computação em nuvem | |
| **Controles possíveis** | **Critérios** |
| Contratos do cliente com provedores de rede devem ser revisados a fim de adequá-los a novos parâmetros, como latência e perda de pacotes, próprios de requisitos das aplicações pretendidas em nuvem | COBIT BAI03 - Manage Solutions Identification and Build; COBIT APO09 - Manage Service Agreements |
| Deve-se buscar garantir que os mecanismos de monitoração das redes consigam distinguir entre problemas internos, na rede dos provedores, ou fora do seu escopo |
| **Risco específico** | |
| 42 - Problemas de dimensionamento de carga da infraestrutura do provedor podem afetar o desempenho dos serviços de computação em nuvem | |
| **Controles possíveis** | **Critérios** |
| OS SLAs com o provedor de nuvem devem ser cuidadosamente definidos e exequíveis, o que inclui penalidades em caso de não cumprimento | COBIT APO10 - Manage Suppliers ; COBIT APO09 - Manage Service Agreements |
| **Risco específico** | |
| 43 - Incompatibilidade entre o modelo arquitetural do cliente e do provedor | |
| **Controles possíveis** | **Critérios** |
| O estudo de viabilidade técnica (estudos técnicos preliminares) da contratação deve avaliar se alternativas de mercado e soluções disponíveis adequam-se à arquitetura do cliente, ou se a adaptação da arquitetura do cliente à do provedor é viável | COBIT BAI03 - Manage Solutions Identification and Build |

# Anexo II - Matriz de auditoria de contratação de serviços de computação em nuvem

|  |  |  |  |
| --- | --- | --- | --- |
| Questão de auditoria | Critérios | Procedimentos | Achados |
| 1. A gestão da segurança da informação, o controle dos ativos e os riscos de segurança relativos à adoção de cloud foram tratados de forma efetiva pela organização? | COBIT DSS04 - Manage Continuity | Verificar a existência de plano de continuidade de negócio do fornecedor | Deficiências nos controles de disponibilidade do serviço de computação em nuvem |
| COBIT DSS04 - Manage Continuity | Verificar a existência de plano de continuidade de negócio do cliente |
| COBIT DSS04 - Manage Continuity | Verificar a compatibilidade entre os planos de continuidade de negócio do cliente e do fornecedor: as premissas de continuidade do cliente precisam estar razoavelmente atendidas nas garantias providas pelo fornecedor |
| COBIT DSS04 - Manage Continuity;  CSA CCM BCR-09 | Verificar que o plano de continuidade de negócio do cliente deve considerar as partes do negócio que estão na nuvem ou que dela dependem, considerando os efeitos de indisponibilidade do serviço em nuvem sobre o negócio e estabelecendo prioridades para recuperação e período máximo tolerável para a indisponibilidade |
| COBIT DSS04 - Manage Continuity | Verificar se o cliente avaliou a possibilidade de selecionar fornecedor que ofereça seus serviços em múltiplas regiões geográficas, para poder transferir serviços de uma região para outra |
| COBIT DSS04 - Manage Continuity | Verificar se o cliente avaliou a possibilidade de selecionar mais de um fornecedor de serviços em nuvem, de forma a ter solução de contingência |
| COBIT DSS04 - Manage Continuity | Verificar se o cliente avaliou a possibilidade de utilizar sua própria infraestrutura de TI como parte da solução de contingência |
| COBIT APO10 - Manage Suppliers;  COBIT APO09 - Manage Service Agreements | Verificar se o contrato com o provedor de nuvem prevê SLAs cuidadosamente definidos e exequíveis, o que inclui penalidades em caso de não cumprimento de parâmetros de disponibilidade dos serviços |

|  |  |  |  |
| --- | --- | --- | --- |
| Questão de auditoria | Critérios | Procedimentos | Achados |
| 1. A gestão da segurança da informação, o controle dos ativos e os riscos de segurança relativos à adoção de cloud foram tratados de forma efetiva pela organização? | COBIT APO13 - Manage Security;  COBIT BAI09 - Manage Assets;  CSA CCM DSI-01 | Verificar se os dados foram submetidos à classificação prévia da informação, antes de serem transmitidos para a nuvem | Deficiências nos controles sobre confidencialidade e integridade dos dados |
| COBIT DSS05 - Manage Security Services;  CSA CCM IAM-02 e IAM-05 | Verificar se foi implementado controle de acesso lógico apropriado ao grau de confidencialidade dos dados armazenados na nuvem |
| COBIT DSS05 - Manage Security Services;  CSA CCM DSI-01 | Verificar a presença de controles para transferência e armazenamento de dados para a nuvem, como criptografia e uso de VPN adequada |
| COBIT DSS05 - Manage Security Services;  CSA CCM EKM-02, EKM-03 e EKM-04 | Verificar que os dados não públicos armazenados no provedor estejam criptografados |
| Verificar que o esquema criptográfico empregado seja adequado à classificação das informações |
| Verificar que as chaves criptográficas não estejam sendo armazenadas na nuvem |
| Verificar que as políticas e procedimentos para uso de criptografia, incluindo gerenciamento de chaves criptográficas estejam estabelecidos e seguidos pelo provedor e pelo cliente |
| COBIT APO09 - Manage Service Agreements;  COBIT APO10 - Manage Suppliers | Verificar se há cláusulas contratuais estabelecendo limites do acesso do provedor aos dados do cliente |
| COBIT DSS05 - Manage Security Services;  CSA CCM DSI-02 | Verificar a existência de controles por parte do provedor para que dados sujeitos a requisitos geográficos não sejam migrados para além de fronteiras definidas em contrato |
| COBIT DSS05 - Manage Security Services | Verificar se as garantias fornecidas pelo provedor demonstram o isolamento de recursos e de dados de seus clientes |

|  |  |  |  |
| --- | --- | --- | --- |
| Questão de auditoria | Critérios | Procedimentos | Achados |
| 1. A gestão da segurança da informação, o controle dos ativos e os riscos de segurança relativos à adoção de cloud foram tratados de forma efetiva pela organização? | COBIT APO09 - Manage Service Agreements;  COBIT APO10 - Manage Suppliers | Verificar se há cláusulas contratuais estabelecendo responsabilidade do provedor em garantir o isolamento de recursos e dados contra acesso indevido por outros clientes | Deficiências nos controles sobre confidencialidade e integridade dos dados |
| COBIT DSS05 - Manage Security | Verificar que o provedor provê controles eficazes e compatíveis com as políticas e procedimentos do cliente para gerenciamento de identidades de usuários e controle de acessos |
| COBIT BAI06 - Manage Changes;  CSA CCM CCC-02 | Verificar a existência de política para gestão de mudanças, que deve ter sido acordada entre provedor e cliente | Falhas nos processos de gestão de mudanças |
| Verificar, no provedor, a existência de processos de gestão de mudanças que incluam comunicação prévia ao cliente acerca de mudanças a serem realizadas |
| COBIT DSS02 - Manage Service Requests and Incidents;  COBIT DSS05 - Manage Security Services; COBIT APO10 - Manage Suppliers;  CSA CCM SEF-02 e SEF-03 | Verificar que os logs de auditoria do provedor registram atividades de acesso de usuários privilegiados, tentativas de acesso autorizados e não autorizados, exceções do sistema e outros eventos de segurança da informação | Falhas na gestão de incidentes de segurança da informação Falhas na auditoria de eventos de segurança da informação |
| Verificar que os logs de eventos de segurança da informação do provedor são mantidos em conformidade com as políticas e regulamentos aplicáveis, e que encontram-se de acordo com as políticas do cliente. |
| Verificar que políticas e procedimentos, definidos em cláusulas contratuais, foram estabelecidos e são seguidos para triagem dos eventos relacionados à segurança, de modo a garantir o gerenciamento de incidentes completo e ágil. |
| Verificar que eventos de segurança de informação são comunicados através de canais predefinidos de comunicação, de maneira rápida e eficiente, e de acordo com os requisitos legais, regulatórios e contratuais |
| COBIT DSS05 - Manage Security Services | Verificar que o cliente realiza cópia dos logs fornecidos pelo provedor, de acordo com sua própria política de retenção |
| Verificar que o provedor fornece mecanismo para filtragem e cópia dos logs gerados pela infraestrutura de nuvem para a área do cliente |

|  |  |  |  |
| --- | --- | --- | --- |
| Questão de auditoria | Critérios | Procedimentos | Achados |
| 1. A gestão da segurança da informação, o controle dos ativos e os riscos de segurança relativos à adoção de cloud foram tratados de forma efetiva pela organização? | CSA CCM IAM-01 | Verificar, no provedor, que o acesso e uso de ferramentas de auditoria que interajam com os sistemas de informação das organizações estejam devidamente segmentados e restritos, a fim de evitar comprometimentos e uso indevido de dados de log | Deficiências nos controles de confidencialidade dos dados Falhas na gestão de incidentes de segurança da informação |
| Verificar se o contrato entre cliente e provedor estabelece direitos claros e exclusivos de propriedade e acesso aos dados, inclusive referentes a logs |
| CSA CCM AIS-01, AIS-02, AIS-03 e AIS-04 | Verificar que o modelo de segurança das interfaces do provedor de computação em nuvem foi desenvolvido com base em padrões de mercado | Falhas na segurança de APIs |
| Verificar que mecanismos de autenticação forte de usuários e controle de acesso para restringir o acesso aos dados do cliente foram implementados |
| COBIT APO10 - Manage Suppliers;  CSA CCM HRS-06, HRS-07, IAM-02, IAM-04, IAM-07 e IAM-09 | Verificar se há definição no contrato de obrigações do provedor quanto a requisitos mínimos de autorização e transparência de acesso do provedor aos ativos físicos e virtuais do cliente, bem como a respeito da necessidade de divulgação ao cliente de suas políticas e orientações específicas | Falhas contratuais relacionadas ao controle de acesso dos ativos físicos e virtuais |
| COBIT APO10 - Manage Suppliers;  CSA CCM HRS-02, HRS-03, HRS-06, HRS-07, HRS-09, IAM-07 e IAM-10 | Verificar a presença no contrato de definições das obrigações do provedor quanto a requisitos mínimos de contratação de pessoal e de monitoramento de suas atividades, bem como a respeito da necessidade de divulgação ao cliente de suas políticas e orientações específicas |
| COBIT DSS05 - Manage Security Services;  CSA CCM TVM-01 e TVM-02 | Verificar que políticas, procedimentos e mecanismos estejam estabelecidos e implementados pelo provedor para gerenciamento de vulnerabilidades conhecidas e atualizações de software, garantindo que aplicações, sistemas e vulnerabilidades de dispositivos de rede sejam avaliadas, e que atualizações de segurança fornecidas sejam aplicadas em tempo hábil, priorizando os patches mais críticos | Falhas na gestão da segurança da informação Falhas nos controles de aplicação de atualizações e correções de segurança |

|  |  |  |  |
| --- | --- | --- | --- |
| Questão de auditoria | Critérios | Procedimentos | Achados |
| 2. Os mecanismos de governança de TI foram revistos, adaptados e implementados adequadamente, de maneira a abranger a adoção de computação em nuvem e gerenciar riscos inerentes à cloud? | COBIT APO02 - Manage Strategy;  COBIT APO08 - Manage Relationships | Verificar se a incorporação de computação em nuvem ao plano estratégico de TI foi precedida de análise adequada de modo a assegurar que serviços de nuvem são a solução mais apropriada para as necessidades da organização | O plano estratégico de TI não contempla aspectos de computação em nuvem Falhas no plano estratégico de TI referentes aos aspectos de computação em nuvem |
| COBIT APO02 - Manage Strategy;  COBIT APO08 - Manage Relationships | Verificar se a incorporação de computação em nuvem ao plano estratégico de TI foi elaborada por um time de profissionais qualificados de TI e de negócio, e se todas as partes interessadas na organização formam consultadas |
| COBIT APO02 - Manage Strategy;  COBIT APO04 - Manage Innovation;  COBIT APO06 - Manage Budget and Costs | Verificar se o planejamento orçamentário está alinhado com as condições de contratação de serviços de computação em nuvem, particularmente quanto à transformação de verba de investimento na compra de equipamentos de TIC para verba de custeio dos serviços de nuvem | Falhas no planejamento orçamentário quanto aos aspectos de computação em nuvem |
| COBIT APO07 - Manage Human Resources;  COBIT APO08 - Manage Relationships | Verificar a existência de política de recursos humanos de TI que contemple redefinições de funções e realocações de pessoal, considerando as capacidades e perfis individuais | Deficiências na política de recursos humanos de TI |
| COBIT APO07 - Manage Human Resources;  COBIT APO08 - Manage Relationships ; COBIT APO04 - Manage Innovation | Verificar a existência de política institucional de incentivo à inovação, como forma de estimular o servidor e quebrar resistência à adoção de computação em nuvem | Deficiências na política institucional de incentivo à inovação |
| CSA CCM GRM-10, AAC-01 e AAC-02 | Verificar se foi prevista em cláusula contratual a necessidade de realização de auditorias por empresas terceiras, com a finalidade de auditar periodicamente a adequação dos controles do provedor em cima de um conjunto de critérios pré-definidos, e fornecer certificados de conformidade baseados nos resultados da auditoria | Falhas contratuais relativas à governança |

|  |  |  |  |
| --- | --- | --- | --- |
| Questão de auditoria | Critérios | Procedimentos | Achados |
| 2. Os mecanismos de governança de TI foram revistos, adaptados e implementados adequadamente, de maneira a abranger a adoção de computação em nuvem e gerenciar riscos inerentes à cloud? | COBIT APO10 - Manage Suppliers | Verificar se foram definidas cláusulas contratuais especificando nível esperado dos serviços (SLA) e mecanismos clássicos de gestão contratual de serviços terceirizados (comunicações formais, multas, rescisão etc) | Falhas contratuais relativas à governança |
| COBIT APO10 - Manage Suppliers | Verificar se foram definidas, no contrato, papéis e responsabilidades do provedor de serviços de nuvem e do cliente |
| COBIT APO10 - Manage Suppliers | Verificar se foram definidas cláusulas contratuais especificando mecanismos de segurança e proteção de propriedade intelectual, e quaisquer requisitos legais ou regulatórios |
| COBIT APO10 - Manage Suppliers | Verificar se foram estabelecidos processos ágeis de contratação e migração para provedores alternativos, em caso de falhas do provedor principal |
| COBIT APO04 - Manage Innovation | Verificar a existência de política institucional de incentivo à inovação de maneira a convertê-la em parte da cultura organizacional | Ausência de política institucional de incentivo à inovação |
| COBIT MEA03 - Ensure Compliance With External Requirements;  CSA CCM AAC-03 | Verificar se a organização é capaz de assegurar a conformidade dos dados e aplicações hospedadas na nuvem com os requisitos de padrões, legais e regulatórios, aos quais o negócio está sujeito, de maneira contínua e atualizada. | Não aderência de dados e aplicações hospedados na nuvem a padrões e legislação pertinentes |
| Decreto 8.135/2013; Portaria Interministerial 141/2014 | Verificar se, na fase de planejamento da contratação, observou-se a possibilidade de enquadramento do objeto como "comunicação de dados da APF" (art. 1º e art. 11 da Portaria Interministerial 141/2014) | Desconformidade, total ou parcial, da contratação de serviços de computação em nuvem aos requisitos legais e normativos brasileiros aplicáveis à APF |
| Portaria Interministerial 141/2014 | Verificar se a organização consultou a disponibilidade dos provedores públicos de atender as especificações técnicas e níveis de serviço do objeto da contratação, até o término da fase de planejamento da contratação (Portaria Interministerial 141/2014, art. 5º, § 3º) |
| Portaria Interministerial 141/2014 | Verificar se a organização observou os requisitos comuns de implementação dos serviços estabelecidos pela Portaria Interministerial 141/2014: padrões do e-Ping (art. 8º) e obrigações que devem estar contidas no termo de referência ou projeto básico e no contrato (art. 9º), especialmente no caso de contratação de fornecedor privado |
| Portaria Interministerial 141/2014 | Verificar que foram observados os requisitos específicos de implementação dos serviços estabelecidos pela Portaria Interministerial 141/2014: requisitos mínimos para serviços de redes de telecomunicações (art. 10) e critérios mínimos de segurança da informação (art. 12), especialmente no caso de contratação de fornecedor privado |

|  |  |  |  |
| --- | --- | --- | --- |
| Questão de auditoria | Critérios | Procedimentos | Achados |
| 2. Os mecanismos de governança de TI foram revistos, adaptados e implementados adequadamente, de maneira a abranger a adoção de computação em nuvem e gerenciar riscos inerentes à cloud? | Portaria Interministerial 141/2014 | Verificar que foram observados os requisitos de auditoria de programas e equipamentos estabelecidos pela Portaria Interministerial 141/2014 (arts. 13 e 14), os quais deverão estar previstos no termo de referência ou projeto básico e no contrato, especialmente no caso de contratação de fornecedor privado | Desconformidade, total ou parcial, da contratação de serviços de computação em nuvem aos requisitos legais e normativos brasileiros aplicáveis à APF |
| Item 4.2.3 da Norma Complementar 19/IN01/DSIC/GSIPR | Verificar que, no caso de infraestrutura de nuvem para sistemas estruturantes da APF, a organização contratou órgão ou entidade da APF |
| Item 5.1 da Norma Complementar 14/IN01/DSIC/GSIPR | Verificar que, antes de adotar a tecnologia de computação em nuvem, a organização observou as diretrizes da sua Política de Segurança da Informação e Comunicações (SIC), do seu processo de Gestão de Riscos de SIC e do seu processo de Gestão de Continuidade de Negócios nos aspectos relacionados à SIC |
| Item 5.2 da Norma Complementar 14/IN01/DSIC/GSIPR | Verificar que, ao contratar ou implementar um serviço de computação em nuvem, a organização verificou que o ambiente, incluindo infraestrutura e canal de comunicação, estava aderente às diretrizes e normas de SIC do GSI/PR, que a legislação brasileira prevaleça e que o contrato de prestação de serviço contenha cláusulas de segurança quanto às informações hospedadas na nuvem |
| Item 5.3 da Norma Complementar 14/IN01/DSIC/GSIPR | Verificar que a organização avaliou quais informações seriam hospedadas na nuvem, considerando o processo de classificação da informação, o valor do ativo de informação, os controles de acesso físicos e lógicos, o modelo de serviço e de implementação de computação em nuvem e a localização geográfica onde as informações seriam armazenadas |

|  |  |  |  |
| --- | --- | --- | --- |
| Questão de auditoria | Critérios | Procedimentos | Achados |
| 3. Foram definidos dispositivos contratuais e mecanismos de gestão contratual adequados para a contratação de serviços de computação em nuvem? | COBIT APO9 - Manage Service Agreements | Verificar se foram previstos e implantados dispositivos contratuais para assegurar os níveis de serviço no caso de interrupções de serviço planejadas ou não planejadas | Falhas contratuais relativas a acordos de níveis de serviço (SLAs) Falhas na gestão contratual relativas a implantação de acordos de níveis de serviço (SLAs) |
| Verificar se foi definido em contrato modelo de remuneração vinculada aos níveis de serviço estabelecidos, prevendo glosas no caso de descumprimento de parâmetros mínimos |
| Verificar se foram definidas em contrato sanções no caso de descumprimento reiterado de parâmetros mínimos de níveis de serviço estabelecidos |
| Verificar se foram previstas soluções de contingência independentes do provedor específico (portabilidade do serviço para outro fornecedor, contrato de contingência em caso de falha do fornecedor principal, espelhamento do serviço em infraestrutura própria etc) | Falhas na gestão de continuidade de negócios |
| COBIT APO9 - Manage Service Agreements; COBIT APO13 - Manage Security | Verificar que há controles para assegurar que todas as vulnerabilidades sejam priorizadas e corrigidas dentro de SLAs acordados contratualmente entre cliente e provedor | Falhas contratuais relativas a acordos de níveis de serviço (SLAs) Falhas na gestão contratual relativas a implantação de acordos de níveis de serviço (SLAs) |
| Avaliar se o processo de gestão de vulnerabilidades do provedor é transparente ao cliente |
| COBIT APO10 - Manage Suppliers | Verificar se foram definidos e implantados no contrato: divisão de papéis entre cliente e provedor; e estabelecimento de indicadores claros e precisos tanto de ambiente como de segurança, com responsáveis pelo seu monitoramento e disponibilização | Falhas contratuais relativas à divisão de responsabilidades entre cliente e provedor  Falhas contratuais no estabelecimento de indicadores Falhas de gestão contratual relativas ao monitoramento de indicadores |
| COBIT APO06 - Manage Budget and Costs | Verificar se foram definidos e utilizados dispositivos contratuais para: verificações intermediárias do nível de uso da capacidade contratada e alertas quando atingidos patamares de recursos e tetos de recursos máximos utilizáveis em função do orçamento disponível; | Falhas de gestão contratual relativas ao monitoramento do nível de uso da capacidade contratada, em função do orçamento disponível |

|  |  |  |  |
| --- | --- | --- | --- |
| Questão de auditoria | Critérios | Procedimentos | Achados |
| 3. Foram definidos dispositivos contratuais e mecanismos de gestão contratual adequados para a contratação de serviços de computação em nuvem? | COBIT BAI03 - Manage Solutions Identification and Build;  CSA CCM IPY-01, IPY-02, IPY-03, IPY-04 e IPY-05 | Verificar que os requisitos da organização para portabilidade e interoperabilidade foram avaliados antes da contratação de nuvem frente às alternativas disponíveis no mercado, a fim de mitigar relações de dependência com o provedor | Falhas contratuais ou de gestão contratual relativas à independência do cliente quanto ao fornecedor (provedor) de computação em nuvem |
| Verificar que foi garantido o uso, pelo provedor, de pacotes modulares, formatos abertos ou populares para dados e serviços |
| Verificar se há transparência por parte do provedor quanto a regulações e taxas aplicadas à transferência de dados |
| Verificar que processos, procedimentos e recursos são estabelecidos e testados, de maneira a viabilizar a transferência de operações de um provedor de computação em nuvem para outro provedor alternativo |
| Especialmente no caso de informações críticas para o negócio, verificar se existe execução de plano de backup independente do fornecedor, duplicando dados em intervalos periódicos |
| Verificar que o contrato prevê condições e limites claros de custos para saída do provedor |
| COBIT APO10 - Manage Suppliers;  COBIT APO12 - Manage Risk;  COBIT BAI03 - Manage Solutions Identification and Build | Verificar se o contrato inclui cláusula especificando que os direitos de propriedade sobre os dados armazenados na nuvem pela organização são exclusivos da organização | Falhas contratuais |
| COBIT BAI03 - Manage Solutions Identification and Build | Verificar se o contrato define em quais países os dados do cliente podem ser armazenados |
| COBIT DSS05 - Manage Security Services | Verificar a existência de dispositivo contratual estabelecendo que o provedor atenda à política de exclusão de dados do cliente |

|  |  |  |  |
| --- | --- | --- | --- |
| Questão de auditoria | Critérios | Procedimentos | Achados |
| 4. Foram abordados e endereçados adequadamente aspectos e processos de gestão relacionados à arquitetura e infraestrutura de computação em nuvem? | COBIT DSS05 - Manage Security Services; COBIT BAI010 - Manage Configuration;  CSA CCM IVS-05, IVS-09 e IPY-05 | Verificar se há dispositivos contratuais que estabeleçam responsabilidades do provedor quanto à implementação de controles para isolamento e segurança de sistema operacional, uso de soluções de virtualização que sejam padrões ou referências de mercado, e política de atualização de versão de *software* e aplicação de correções | Falhas relativas à infraestrutura de TI |
| COBIT APO09 - Manage Service Agreements;  COBIT APO10 - Manage Suppliers;  COBIT DSS02 - Manage Service Requests and Incidents;  CSA CCM SEF-02, SEF-03 e STA-02 | Verificar se o contrato detalha definições específicas de incidentes, eventos, ações a serem tomadas e responsabilidades do provedor e do cliente |
| Verificar se o contrato define requisitos de interoperabilidade entre as ferramentas de gestão de incidentes do provedor e do cliente |
| COBIT BAI03 - Manage Solutions Identification and Build;  COBIT APO09 - Manage Service Agreements | Verificar se os contratos do cliente com seus provedores de rede foram revisados a fim de adequá-los a novos parâmetros, como latência e perda de pacotes, próprios de requisitos das aplicações pretendidas em nuvem |
| Verificar se há mecanismos de monitoração das redes que consigam distinguir entre problemas internos, na rede dos provedores, ou fora do seu escopo |
| COBIT APO10 - Manage Suppliers;  COBIT APO09 - Manage Service Agreements | Verificar se o contrato com o provedor de nuvem prevê SLAs cuidadosamente definidos e exequíveis, o que inclui penalidades em caso de não cumprimento de parâmetros de desempenho dos serviços |
| COBIT BAI03 - Manage Solutions Identification and Build | Verificar se o estudo de viabilidade técnica (estudos técnicos preliminares) da contratação avaliou a adequação de alternativas de mercado e soluções disponíveis à arquitetura do cliente, ou se a adaptação da arquitetura do cliente à do provedor é viável |

# Anexo III - Conceitos correlatos

# 1. Computação em nuvem e virtualização

1. Os termos “computação em nuvem” e “virtualização” têm sido intrinsecamente associados e,muitas vezes, utilizados como sinônimos. Apesar de computação em nuvem não ser sinônimo de virtualização, atualmente as tecnologias de virtualização são as que sustentam qualquer forma de implantação de nuvem.

2. A arquitetura dos computadores servidores atuais foi inicialmente projetada para funcionar com apenas um sistema operacional e um aplicativo por vez. Como resultado, até mesmo *data centers* pequenos precisam utilizar muitos servidores, cada um operando com apenas parte pequena de sua capacidade de processamento. A tecnologia de virtualização resolve esse problema ao permitir a execução de vários sistemas operacionais e aplicativos em um mesmo computador servidor, possibilitando a utilização de sua capacidade total[[1]](#endnote-1).

3. A virtualização isoladamente não provê todas as características definidas pelo NIST para a computação em nuvem, como o autoprovisionamento e a rápida elasticidade. Os usuários não podem, simplesmente, criar máquinas virtuais de acordo com suas necessidades sem interação com a área de TI. Apesar da flexibilidade associada à virtualização, os recursos disponíveis para provisionamento não podem ser alocados a qualquer hora e em qualquer volume.

4. Como a virtualização serve para tornar os ambientes computacionais independentes de *hardware*, um ambiente totalmente virtualizado é um primeiro passo na direção de se implantar uma nuvem, seja ela pública, privada ou híbrida. Apesar da virtualização de servidores ser a mais consolidada nas organizações, há que se pensar nela de maneira mais ampla, abrangendo outros ativos de TI, como armazenamento e rede.

5. Se uma instituição já conseguiu virtualizar todo seu parque computacional, a transição para uma nuvem privada se dará pela adição de uma camada de orquestração e de um catálogo de serviços, o que claramente irá requerer organização e planejamento minucioso.

# 2. Automação e Orquestração

6. Segundo a revista Information Week*[[2]](#endnote-2)*, “automação é a fundação sobre a qual se constrói a orquestração” (tradução livre). Trata-se de processos programados que automatizam tarefas repetitivas. Um exemplo de um processo que é facilmente automatizado é o provisionamento de servidores virtuais.

7. Já a orquestração utiliza a automação de processos como base. É um software que vincula vários produtos, tecnologias e processos para permitir a automação de TI fim a fim, cujo gerenciamento tipicamente ocorre por meio de um portal.

8. Há, no mercado, muitos fornecedores vendendo ferramentas de orquestração para provimento de nuvens privadas ou híbridas como se fossem soluções de computação em nuvem, mas que são, na verdade, soluções para provimento de infraestrutura para computação em nuvem.

# 3. Nuvem gerenciada

9. Além das classificações expostas anteriormente, ainda há o conceito de “nuvem gerenciada” (*managed cloud*). Trata-se de solução de computação em nuvem associada a serviços de gerenciamento e operação. Esta terminologia está em crescente uso pelos provedores de serviços de TI, apesar de não ser ainda difundida na literatura. Os serviços de gerenciamento de nuvem adicionam itens de serviços ao que tradicionalmente é ofertado, como por exemplo: *backups* de dados, gerenciamento a nível de sistema operacional e aplicação, monitoramento e suporte técnico para sistemas operacionais e aplicações. Eles também alteram a fronteira de responsabilidades apresentada na Figura 4, aumentando as camadas gerenciadas pelo provedor, e, consequentemente, diminuindo o que é gerenciado pelo cliente ou consumidor.

# 4. Collocation e serviços gerenciados

10. A revista *online* Networkworld, em um artigo sobre serviços gerenciados de nuvem*[[3]](#endnote-3)*, afirma que (tradução livre):

O movimento para se ter mais aspectos gerenciados do mercado de nuvem é natural. A nuvem cresceu a partir da indústria de serviços gerenciados, o qual, por sua vez, originou-se do mercado de *collocation*. As diferenças entre estas ofertas são pequenas, mas importantes:

1) *Collocation*: Os fornecedores de *collocation* provêm as instalações físicas do *data center*, a energia e o ar condicionado, mas a propriedade e a gerência da infraestrutura de TI são dos clientes;

2) Serviços Gerenciados: Os fornecedores provêm a infraestrutura inteira que é dedicada aos clientes individuais, os quais gerenciam desde o sistema operacional até a aplicação;

3) Nuvem: É uma forma ainda mais automatizada de serviços gerenciados, na qual clientes acessam recursos hospedados sob demanda através de um portal *web* ou uma API (*Application Programming Interface*);

4) Nuvem gerenciada: Adiciona uma nova camada ao topo de todos estes serviços, com os recursos de nuvem sendo gerenciados de maneira mais ativa e interventiva por parte do fornecedor.

11. Tanto os serviços de collocation quanto os serviços gerenciados não são serviços de computação em nuvem, pois não apresentam todas as características definidas pelo NIST.

# 5. XaaS

12. É frequente encontrar na internet outros tipos de serviço de computação em nuvem comercializados como XaaS (“*Anything as a Service*”, ou em português, “Tudo como Serviço”), onde a letra “X” da sigla pode ser trocada pela inicial do serviço sendo ofertado. Apesar do XaaS ser rotulado como mais uma estratégia de *marketing*, ele está aderente ao conceito de utilização de várias camadas de abstração – neste sentido, qualquer serviço específico pode fazer parte de uma nova categoria, e ainda assim, basear-se em serviços das camadas inferiores.

13. Um exemplo de XaaSé o DaaS, ou Desktop *as a Service*, descrito no site *CloudTech[[4]](#endnote-4)*. Em um serviço de *desktop* na nuvem, o provedor precisará disponibilizar de pelo menos duas camadas na nuvem:

1) servidores para rodar infraestrutura de *desktop virtual* de um provedor de *IaaS*, e os serviços de manutenção e atualização dos equipamentos associados;

2) um pacote de *office*, como o Microsoft Office 365 (SaaS).

14. Serão necessários, também, serviços de manutenção e aplicação de *patches* de sistema operacional, e um terminal de acesso*.* O provedor de DaaS será responsável por desenhar a solução, montá-la e gerenciá-la.

1. VMWARE.COM. Noções básicas da virtualização. Disponível em: <<http://www.vmware.com/br/virtualization/virtualization-basics/what-is-virtualization.html>​>. Acessado em: 18/03/2015. [↑](#endnote-ref-1)
2. ONISICK, J. *Cloud Infrastructure*: Private Cloud Automation, Orchestration, And Measured Service. InformationWeek Network Computing, 06/23/2011. Disponível em: <http://www.networkcomputing.com/

   cloud-infrastructure/private-cloud-automation-orchestration-and-measured-service/a/d-id/123284

   1?page\_number=1>. Acessado em: 04/11/2014. [↑](#endnote-ref-2)
3. BUTLER, B. *Rackspace rolls out new hosted computing tier: Managed cloud*. Net Work World, 15/07/2014. Disponível em: <http://www.networkworld.com/article/2454284/cloud-computing/r

   ackspace-rolls-out-new-hosted-computing-tier-managed-cloud.html>. Acessado em: 03/11/2014. [↑](#endnote-ref-3)
4. DIXON, J. *X as a service (XaaS):* What the future of cloud computing will bring. Cloudtech. GreenPages Technology Solutions, 18/08/2014. Disponível em: <http://www.cloudcomputing-news.net/news/2014/aug/18/x-as-a-service-xaas-what-the-future-of-cloud-computing-will-bring/>. Acessado em: 04/11/2014. [↑](#endnote-ref-4)