INFRA S.A.
ASSEMBLEIA GERAL
CONSELHO DE ADMINISTRAÇÃO
DIRETORIA EXECUTIVA
DIRETORIA DE MERCADO E INOVAÇÃO
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO
GERÊNCIA DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO

# ANEXO X

Brasília, 16 de dezembro de 2024.

## HISTÓRICO DE REVISÕES

| Data | Versão | Descrição | Autor |
|---|---|---|---|
| 22/09/2024 | 1.0 | Finalização da primeira versão do documento | Equipe de Planejamento |

## ANEXO X - IDENTIFICAÇÃO E ANÁLISE DOS RISCOS ENVOLVIDOS

### 1. MATRIZ DE RISCO CONTRATUAL

| CATEGORIA DO RISCO | DESCRIÇÃO | CONSEQUÊNCIA | MITIGAÇÃO | ALOCAÇÃO |
|---|---|---|---|---|
| **Execução** | Atraso na execução do objeto por culpa do Contratado. | Aumento do custo do serviço. | Diligência do Contratado na execução contratual. | **Contratado** |
| | Fatos retardadores ou impeditivos da execução do objeto próprios do risco ordinário da atividade empresarial ou da execução. | Aumento do custo do serviço. | Planejamento empresarial. | **Contratado** |

| CATEGORIA DO RISCO | DESCRIÇÃO | CONSEQUÊNCIA | MITIGAÇÃO | ALOCAÇÃO |
|---|---|---|---|---|
| | Fatos retardadores ou impeditivos da execução do objeto que não estejam na sua álea ordinária, tais como fatos do príncipe, caso fortuito ou de força maior, bem como o retardamento determinado pela Contratante, que comprovadamente repercuta no preço do Contratado. | Aumento do custo do serviço. | Revisão de preço. | **Contratante** |
| **Risco da Atividade Empresarial** | Alteração de enquadramento tributário, em razão do resultado ou de mudança da atividade empresarial, bem como por erro do Contratado na avaliação da hipótese de incidência tributária. | Aumento ou diminuição do lucro do Contratado. | Planejamento tributário. | **Contratado** |
| | Elevação de gastos com viagens superiores ao estimado pelo Contratado. | Aumento do custo do serviço. | Melhor planejamento contratual. | **Contratado** |
| | Elevação dos custos operacionais para o desenvolvimento da atividade empresarial em geral e para a execução do objeto em particular, tais como aumento de preço de insumos, prestadores de serviço e mão de obra. | Aumento do custo do serviço. | Reequilíbrio econômico-financeiro. | **Contratante** |

| CATEGORIA DO RISCO | DESCRIÇÃO | CONSEQUÊNCIA | MITIGAÇÃO | ALOCAÇÃO |
|---|---|---|---|---|
| | Elevação dos custos operacionais definidos na linha anterior, quando superior ao índice de reajuste previsto na Cláusula de Equilíbrio Econômico-Financeiro do Contrato. | Aumento do serviço. | Reequilíbrio econômico-financeiro. | **Contratado** |
| **Riscos Trabalhista e Previdenciário** | Responsabilização da Contratante por verbas trabalhistas e previdenciárias dos profissionais do Contratado alocados na execução do objeto contratual. | Geração de custos trabalhistas e/ou previdenciários para a Contratante, além de eventuais honorários advocatícios, multas e verbas sucumbenciais. | Ressarcimento, pelo Contratado, ou retenção de pagamento e compensação com valores a este devidos, da quantia despendida pela Contratante. | **Contratado** |
| **Risco Tributário e Fiscal (Não Tributário).** | Responsabilização da Infra S.A. por recolhimento indevido em valor menor ou maior que o necessário, ou ainda de ausência de recolhimento, quando devido, sem que haja culpa da Infra S.A. | Débito ou crédito tributário ou fiscal (não tributário). | Ressarcimento, pelo Contratado, ou retenção de pagamento e compensação com valores a este devidos, da quantia dispendida pela Contratada. | **Contratado** |

## 2. MAPA DE GERENCIAMENTO DE RISCOS

### 2.1. Preliminares

O gerenciamento de riscos* permite ações contínuas de planejamento, organização e controle dos recursos relacionados aos riscos que possam comprometer o sucesso da contratação, da execução do objeto e da gestão contratual.

O Mapa de Gerenciamento de Riscos deve conter a identificação e a análise dos principais riscos, consistindo na compreensão da natureza e determinação do nível de risco, que corresponde à combinação do impacto e de suas probabilidades que possam comprometer a efetividade da contratação, bem como o alcance dos resultados pretendidos com a solução de TIC.

Para cada risco identificado, define-se: a probabilidade de ocorrência dos eventos, os possíveis danos e impacto caso o risco ocorra, possíveis ações preventivas e de contingência (respostas aos riscos), a identificação de responsáveis pelas ações, bem como o registro e o acompanhamento das ações de tratamento dos riscos.

Os riscos identificados no projeto devem ser registrados, avaliados e tratados:

Durante a fase de planejamento, a equipe de Planejamento da Contratação deve proceder às ações de gerenciamento de riscos e produzir o Mapa de Gerenciamento de Riscos;

Durante a fase de Seleção do Fornecedor, o Integrante Administrativo com apoio dos Integrantes Técnico e Requisitante deve proceder às ações de gerenciamento dos riscos e atualizar o Mapa de Gerenciamento de Riscos;

Durante a fase de Gestão do Contrato, a Equipe de Fiscalização do Contrato, sob coordenação do Gestor do Contrato, deverá proceder à atualização contínua do Mapa de Gerenciamento de Riscos, procedendo à reavaliação dos riscos identificados nas fases anteriores com a atualização de suas respectivas ações de tratamento, e a identificação, análise, avaliação e tratamento de novos riscos.

| Classificação | Valor |
|---|---|
| Baixo | 5 |
| Médio | 10 |
| Alto | 15 |

Tabela 1: Escala de classificação de probabilidade e impacto.

A tabela a seguir apresenta a Matriz Probabilidade x Impacto, instrumento de apoio para a definição dos critérios de classificação do nível de risco.

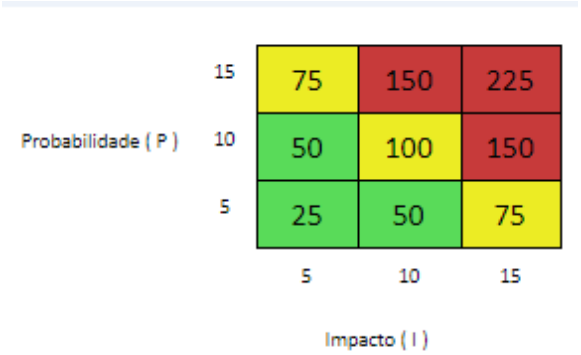


Figura 1: Matriz Probabilidade x Impacto

***Referência: Art. 38 IN SGD/ME nº 94, de 2022.**

## 2.2. Identificação dos Riscos

I - A tabela a seguir apresenta uma síntese dos riscos identificados e classificados neste documento.

| Id | Risco | Relacionado ao(à): [1] | P [2] | I [3] | Nível de Risco (P x I) [4] |
|---|---|---|---|---|---|
| **R01** | Informação de volume de serviço incompatível com a realidade da INFRA S.A., levando a uma super estimativa dos volumes com a geração de expectativa irreal para o mercado. | **PC** | 5 | 10 | **50** |
| **R02** | Atrasos na conclusão da contratação. | **PC SF** | 5 | 15 | **75** |
| **R03** | Selecionar fornecedor inadequado para execução do contrato. | **PC** | 5 | 15 | **75** |
| **R04** | Contratação com preço acima da média do mercado. | **PC SF** | 5 | 15 | **75** |
| **R05** | Falta de qualificação dos profissionais responsáveis pela gestão e fiscalização do contrato. | **GC** | 10 | 15 | **150** |
| **R06** | Desconformidade de execução contratual. | **GC** | 5 | 15 | **75** |
| **R07** | Pagamento indevido. | **GC** | 5 | 15 | **75** |

| | | | | | |
|---|---|---|---|---|---|
| **R08** | Ausência de garantia contratual válida. | **GC** | 5 | 10 | **50** |
| **R09** | Dificuldades técnicas na transição contratual. | **GC** | 5 | 15 | **75** |
| **R10** | Finalização antecipada do contrato. | **GC** | 5 | 15 | **75** |
| **R11** | Dependência técnica elevada da equipe da Infra S.A. em relação aos profissionais da contratada. | **GC** | 5 | 10 | **50** |
| **R12** | A Contratada não cumpre os níveis mínimos de serviço acordados. | **GC** | 10 | 15 | **150** |
| **R13** | Falhas na disponibilidade dos serviços de nuvem. | **GC** | 15 | 15 | **225** |
| **R14** | Vazamento de dados ou acesso não autorizado. | **GC** | 10 | 15 | **150** |
| **R15** | Violação da legislação e normativos da INFRA S.A. | **GC** | 5 | 15 | **75** |
| **R16** | Aumento inesperado nos custos devido a serviços adicionais ou mudanças de escopo. | **GC** | 10 | 10 | **100** |
| **R17** | Dificuldades na integração e gestão de múltiplos provedores. | **GC** | 10 | 15 | **150** |
| **R18** | Suporte técnico inadequado ou lento. | **GC** | 15 | 10 | **150** |
| **R19** | Dificuldades ou falhas na migração de dados e serviços para a nova plataforma. | **GC** | 10 | 15 | **150** |

*Legenda: P – Probabilidade; I – Impacto.*

*[1] A qual natureza o risco está associado: fases do Processo da Contratação ou Solução.*

*[2] Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).*

*[3] Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).*

*[4] Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).*

## 2.3. Avaliação e Tratamento dos Riscos Identificados

| | | |
|---|---|---|
| **Risco:** | **R05 - Falta de qualificação dos profissionais responsáveis pela gestão e fiscalização do contrato.** | |
| **Probabilidade:** | Médio | |
| **Impacto:** | Alto | |
| **Dano 1:** | Deixar de executar ou executar de forma ineficiente a gestão e fiscalização do contrato. | |
| **Tratamento:** | Mitigar | |
| **Id** | **Ação Preventiva** | **Responsável** |
| 1 | Providenciar treinamento para gestores e fiscais de contrato. | Superintendência de Gestão de Pessoas - SUGEP |
| **Id** | **Ação de Contingência** | **Responsável** |

| | | | |
|---|---|---|---|
| **Risco 05** | 1 | **Substituir profissional: s**ubstituir profissionais com treinamento insuficiente por outros mais capazes. | • Área Requisitante<br>• Diretoria Requisitante<br>• Alta Administração |
| | 2 | **Escalonamento rápido:** escalonar rapidamente, caso surjam problemas ou entraves que afetem os prazos. | • Área Requisitante<br>• Diretoria Requisitante<br>• Alta Administração |
| | 3 | **Equipe reserva:** identificar e alocar equipe de reserva para substituição pronta para intervir, caso algum membro principal fique indisponível, para garantir que o processo continue sem interrupções significativas. | • Área Requisitante<br>• Diretoria Requisitante<br>• Alta Administração |

| | | | |
|---|---|---|---|
| | **Risco:** | **R12 - A Contratada não cumpre os níveis mínimos de serviço acordados.** | |
| | **Probabilidade:** | Médio | |
| | **Impacto:** | Alto | |
| | **Dano 1:** | Redução da qualidade dos serviços prestados, afetando a operação e a satisfação dos usuários. | |
| | **Dano 2:** | Possível interrupção de processos críticos e impacto financeiro devido à necessidade de correção ou substituição dos serviços. | |
| | **Tratamento:** | Mitigar | |
| | **Id** | **Ação Preventiva** | **Responsável** |
| | 1 | Estabelecer SLAs (Service Level Agreements) claros e métricas de desempenho | Área Requisitante |
| | 2 | Monitorar o desempenho regularmente e aplicar penalidades contratuais por não conformidade. | Área Requisitante |
| | **Id** | **Ação de Contingência** | **Responsável** |

| | | | |
|---|---|---|---|
| **Risco 12** | 1 | **Desenvolver um plano de recuperação de desastres específico para a interrupção de serviços:** criar um plano detalhado que inclua procedimentos para restaurar os serviços críticos, identificar responsabilidades e recursos necessários para uma recuperação eficaz. | • Área Requisitante<br>• Diretoria Requisitante<br>• Alta Administração |
| | 2 | **Identificar e negociar com fornecedores alternativos para serviços críticos:** ter fornecedores alternativos prontos para entrar em ação caso o serviço atual falhe, garantindo uma transição suave e minimizando o impacto. | • Área Requisitante<br>• Diretoria Requisitante<br>• Alta Administração |
| | 3 | **Estabelecer um procedimento de comunicação de emergência para manter os usuários informados durante a interrupção:** criar um protocolo para comunicar rapidamente os usuários finais sobre a situação e fornecer atualizações regulares até a resolução do problema. | • Área Requisitante<br>• Diretoria Requisitante<br>• Alta Administração |

| | | |
|---|---|---|
| | **Risco:** | **R13 - Falhas na disponibilidade dos serviços de nuvem.** |
| | **Probabilidade:** | Alto |
| | **Impacto:** | Alto |
| | **Dano 1:** | Indisponibilidade dos serviços e aplicações, resultando em perda de produtividade e possíveis interrupções de trabalho. |
| | **Dano 2:** | Interrupção dos processos de negócios da INFRA S.A., levando a perdas financeiras, impacto na reputação e comprometimento da satisfação dos clientes. |

| | | | |
|---|---|---|---|
| **Risco 13** | **Tratamento:** | Mitigar | |
| | **Id** | **Ação Preventiva** | **Responsável** |
| | 1 | Garantir cláusulas de uptime e redundância no contrato com o provedor de nuvem. | Área Requisitante |
| | 2 | Implementar monitoramento contínuo dos serviços e criar um plano de recuperação de desastres para minimizar o impacto de falhas. | Área Requisitante e Alta Administração |
| | **Id** | **Ação de Contingência** | **Responsável** |
| | 1 | **Ativar o plano de recuperação de desastres**: acionar procedimentos detalhados para restaurar os serviços interrompidos, com o objetivo de minimizar o tempo de inatividade e a perda de dados. O plano deve incluir a alocação de recursos, definição de prioridades e etapas específicas para a recuperação dos serviços afetados. | • Área Requisitante<br>• Diretoria Requisitante<br>• Alta Administração |

| | | | |
|---|---|---|---|
| | 2 | **Mobilizar fornecedores alternativos ou serviços de nuvem secundários**: ter contratos e acordos com fornecedores alternativos que podem fornecer serviços de forma rápida, caso o fornecedor principal falhe, garantindo a continuidade dos processos críticos. A INFRA S.A. deverá manter uma lista atualizada de fornecedores alternativos, bem como estabelecer acordos sobre prazos de ativação e níveis de serviço. | • Área Requisitante<br>• Diretoria Requisitante<br>• Alta Administração |
| | 3 | **Estabelecer e executar um plano de comunicação**: informar os usuários e partes interessadas sobre a situação, oferecendo atualizações regulares e instruções sobre como proceder durante a falha. | • Área Requisitante<br>• Diretoria Requisitante<br>• Alta Administração |

| | | |
|---|---|---|
| | **Risco:** | **R14 - Vazamento de dados ou acesso não autorizado.** |
| | **Probabilidade:** | Médio |
| | **Impacto:** | Alto |
| | **Dano 1:** | Exposição de dados sensíveis ou confidenciais, o que pode levar a danos à reputação da Infra S.A. e à perda de confiança dos clientes. |
| | **Dano 2:** | Potenciais penalidades financeiras e legais devido à violação de regulamentos de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD). |
| | **Tratamento:** | Mitigar |

| | | |
|---|---|---|
| **Id** | **Ação Preventiva** | **Responsável** |

| | | | |
|---|---|---|---|
| | 1 | Implementar criptografia de dados em trânsito e em repouso e garantir controles de acesso baseados em privilégios mínimos. Revisar e reforçar a segurança de autenticação e autorização. | Área Requisitante |
| | 2 | Conduzir auditorias internas e externas regulares para identificar falhas de segurança e vulnerabilidades. Aplicar correções e atualizar medidas de segurança conforme necessário. | Área Requisitante e Alta Administração |
| | **Id** | **Ação de Contingência** | **Responsável** |
| **Risco 14** | 1 | **Acionar o plano de resposta a incidentes de segurança**: implementar procedimentos definidos para conter o incidente, minimizar os danos e restaurar a segurança dos dados afetados, contendo a identificação da origem do vazamento e a realização de ações corretivas imediatas. | • Área Requisitante<br>• Diretoria Requisitante<br>• Alta Administração |

| | | | |
|---|---|---|---|
| | 2 | **Notificar as partes afetadas e autoridades regulatórias**: informar os indivíduos cujos dados foram comprometidos e as autoridades relevantes de acordo com as leis e regulamentos de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) e os normativos internos da INFRA S.A. | • Área Requisitante<br>• Diretoria Requisitante<br>• Alta Administração |
| | 3 | **Revisar e atualizar políticas de segurança e controles de acesso**: analisar o incidente para identificar falhas e melhorar as políticas e controles para prevenir futuros incidentes, tais como a implementação de melhorias baseadas nas lições aprendidas. | • Área Requisitante<br>• Diretoria Requisitante<br>• Alta Administração |

| | | | |
|---|---|---|---|
| | **Risco:** | **R17 - Dificuldades na integração e gestão de múltiplos provedores.** | |
| | **Probabilidade:** | Médio | |
| | **Impacto:** | Alto | |
| | **Dano 1:** | Interrupção nos serviços e operações devido a falhas na integração, afetando a continuidade dos negócios e a disponibilidade das aplicações. | |
| | **Dano 2:** | Custo adicional e perda de eficiência devido a problemas de comunicação e compatibilidade entre provedores. | |
| | **Tratamento:** | Mitigar | |
| | **Id** | **Ação Preventiva** | **Responsável** |
| | 1 | Definir claramente a responsabilidade do cloud broker e a coordenação entre provedores. | Área Requisitante<br>Diretoria Requisitante<br>Alta Administração |

| | | | |
|---|---|---|---|
| | | Estabelecer processos de integração e comunicação eficazes para garantir a compatibilidade entre diferentes provedores e evitar falhas na migração. | Área Requisitante<br>Alta Administração |
| **Risco 17** | **Id** | **Ação de Contingência** | **Responsável** |
| | 1 | **Acionar um plano de suporte técnico**: ter uma equipe de suporte técnico pronta para intervir e resolver rapidamente problemas que possam surgir durante a integração e migração, minimizando o impacto e tempo de inatividade. | • Área Requisitante<br>• Diretoria Requisitante<br>• Alta Administração |
| | 2 | **Implementar backups regulares e criar um plano de rollback**: garantir que dados críticos sejam periodicamente salvos e que haja um plano para reverter mudanças em caso de falhas, com objetivo de proteger contra perda de dados e facilitar a recuperação após problemas. | • Área Requisitante<br>• Diretoria Requisitante<br>• Alta Administração |

| | | | |
|---|---|---|---|
| | 3 | **Realizar uma revisão pós-migração**: após a migração e integração, avaliar o processo e identificar problemas que possam ter ocorrido, bem como verificar a integridade dos dados e a eficiência dos novos processos, e fazer ajustes necessários para melhorar a operação. | • Área Requisitante<br>• Diretoria Requisitante<br>• Alta Administração |

| | | | |
|---|---|---|---|
| | **Risco:** | **R18 - Suporte técnico inadequado ou lento.** | |
| | **Probabilidade:** | Alto | |
| | **Impacto:** | Médio | |
| | **Dano 1:** | Interrupção de operações e perda de produtividade devido a problemas técnicos não resolvidos rapidamente. | |
| | **Dano 2:** | Aumento de custos operacionais pela necessidade de soluções alternativas ou suporte adicional. | |
| | **Tratamento:** | Mitigar | |
| | **Id** | **Ação Preventiva** | **Responsável** |
| | 1 | Estabelecer acordos de nível de serviço (SLAs) com prazos de resposta e resolução claros e exigir que os provedores de suporte cumpram esses SLAs. | Área Requisitante |
| | 2 | Acionar uma equipe interna ou um suporte técnico alternativo, caso o suporte técnico do provedor seja inadequado ou lento, ter uma equipe interna ou um fornecedor alternativo pronto para resolver problemas críticos rapidamente. | Área Requisitante |
| | **Id** | **Ação de Contingência** | **Responsável** |

| | | | |
|---|---|---|---|
| **Risco 18** | 1 | **Acionar uma equipe interna ou um suporte técnico alternativo**: caso o suporte técnico do provedor seja inadequado ou lento, ter uma equipe interna ou um fornecedor alternativo pronto para resolver problemas críticos rapidamente. | • Área Requisitante<br>• Diretoria Requisitante<br>• Alta Administração |
| | 2 | **Implementar um processo de escalonamento**: estabelecer um protocolo claro para escalar problemas críticos que não são resolvidos dentro dos prazos acordados, garantindo que a alta administração esteja envolvida na resolução de questões graves. | • Área Requisitante<br>• Diretoria Requisitante<br>• Alta Administração |
| | 3 | **Realizar avaliações regulares do desempenho do suporte técnico**: monitorar e avaliar periodicamente a eficácia do suporte técnico recebido. Com base nas avaliações, ajustar contratos ou mudar de provedor se necessário para melhorar o suporte. | • Área Requisitante<br>• Diretoria Requisitante<br>• Alta Administração |

| | | | |
|---|---|---|---|
| | **Risco:** | | **R19 - Dificuldades ou falhas na migração de dados e serviços para a nova plataforma.** |
| | **Probabilidade:** | | Médio |
| | **Impacto:** | | Alto |
| | **Dano 1:** | | Interrupção dos serviços e operações devido a falhas na migração, afetando a continuidade dos negócios. |
| | **Dano 2:** | | Perda de dados e integridade, resultando na perda de informações críticas e afetando a precisão dos dados. |
| | **Tratamento:** | | Mitigar |
| | **Id** | **Ação Preventiva** | **Responsável** |

| | | | |
|---|---|---|---|
| | 1 | Realizar um planejamento detalhado da migração, incluindo testes de compatibilidade e desempenho, e criar um cronograma realista. | Área Requisitante |
| | 2 | Executar um piloto ou teste de migração em um ambiente controlado para identificar e resolver problemas antes da migração completa. | Área Requisitante |
| | **Id** | **Ação de Contingência** | **Responsável** |
| **Risco 19** | 1 | **Acionar um plano de recuperação**: ter um plano de contingência para reverter para a plataforma anterior em caso de falhas significativas durante a migração, com o objetivo de minimizar a interrupção dos serviços e a recuperação rápida. | • Área Requisitante<br>• Diretoria Requisitante<br>• Alta Administração |
| | 2 | **Restaurar dados a partir de backups**: garantir que existam backups atualizados dos dados para permitir a restauração em caso de problemas durante a migração, com vista a proteger contra a perda de dados críticos. | • Área Requisitante<br>• Diretoria Requisitante<br>• Alta Administração |

| | | | |
|---|---|---|---|
| | 3 | **Estabelecer uma equipe de suporte**: ter uma equipe dedicada para resolver problemas rapidamente durante e após a migração, garantindo uma resposta eficiente e minimizando o tempo de inatividade. | • Área Requisitante<br>• Diretoria Requisitante<br>• Alta Administração |

## 3. RISCOS ESPECÍFICOS E CONTROLES POSSÍVEIS (ACÓRDÃO 1739/2015 TCU PLENÁRIO)

3.1. **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.

3.1.1. **Controles Possíveis:**

3.1.1.1. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de um plano de continuidade que abranja todas as partes do negócio, incluindo aquelas na nuvem (Item 4.2.3).
- Evidência 2: O Termo de Referência destaca a importância de considerar as características do provedor de nuvem na elaboração do plano de continuidade (Item 5.1).
- Evidência 3: O Anexo II - Especificações Técnicas reforça a necessidade de um plano de continuidade que leve em conta as especificidades do provedor de nuvem (Item 5.2).

3.1.1.2. Considerar capacidade do provedor de trabalhar com multirregiões no provedor e poder transferir carga de uma região para outra.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a capacidade de transferência de carga entre regiões como um critério importante (Item 5.3).
- Evidência 2: O Termo de Referência inclui requisitos para que o provedor de nuvem tenha capacidade de operar em múltiplas regiões (Item 5.4).
- Evidência 3: O Anexo II - Especificações Técnicas detalha as especificações técnicas para a transferência de carga entre regiões (Item 5.5).

3.1.1.3. O plano de continuidade de negócio para nuvem pode considerar mais de um provedor como contingência.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) sugere a utilização de múltiplos provedores como uma estratégia de contingência (Item 5.6).
- Evidência 2: O Termo de Referência recomenda a consideração de mais de um provedor para garantir a continuidade do negócio (Item 5.7).

- Evidência 3: O Anexo II - Especificações Técnicas menciona a possibilidade de utilizar múltiplos provedores como parte do plano de continuidade (Item 5.8).

3.1.1.4. Considerar a alternativa de utilizar sua própria infraestrutura de TI como contingência.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) discute a utilização da infraestrutura própria como uma opção de contingência (Item 5.9).
- Evidência 2: O Termo de Referência inclui a infraestrutura própria como uma alternativa viável (Item 5.10).
- Evidência 3: O Anexo II - Especificações Técnicas detalha as especificações para a utilização da infraestrutura própria como contingência (Item 5.11).

3.1.1.5. Os SLAs com o provedor de nuvem devem ser cuidadosamente definidos e exequíveis, o que inclui penalidades em caso de não cumprimento.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) enfatiza a importância de definir SLAs claros e exequíveis (Item 5.12).
- Evidência 2: O Termo de Referência detalha os requisitos para SLAs com penalidades em caso de não cumprimento (Item 5.13).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de SLAs bem definidos e com penalidades (Item 5.14).

3.2. **Risco Específico 2:** Indisponibilidade de elementos da infraestrutura do cliente que são críticos para o acesso a serviços na nuvem.

3.2.1. **Controles Possíveis:**

3.2.1.1. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de um método documentado para determinar o impacto da indisponibilidade (Item 6.1).
- Evidência 2: O Termo de Referência destaca a importância de estabelecer prioridades para recuperação (Item 6.2).
- Evidência 3: O Anexo II - Especificações Técnicas reforça a necessidade de definir um período máximo tolerável para a indisponibilidade (Item 6.3).

3.3. **Risco Específico 3:** Controle de acesso inexistente ou insuficiente para assegurar a confidencialidade dos dados armazenados na nuvem.

3.3.1. **Controles Possíveis:**

3.3.1.1. Os dados devem ser submetidos à classificação prévia da informação, antes de serem transmitidos para a nuvem.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a classificação prévia da informação como uma medida

essencial (Item 7.1).

- Evidência 2: O Termo de Referência inclui a classificação prévia da informação como um requisito (Item 7.2).
- Evidência 3: O Anexo II - Especificações Técnicas detalha as especificações para a classificação prévia da informação (Item 7.3).

3.3.1.2. Implementar controle de acesso lógico apropriado ao grau de confidencialidade dos dados armazenados na nuvem.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a implementação de controles de acesso lógico (Item 7.4).
- Evidência 2: O Termo de Referência detalha os requisitos para controles de acesso (Item 7.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de controles de acesso lógico (Item 7.6).

3.4. **Risco Específico 4:** A segurança dos dados transmitidos para o provedor de nuvem pela internet pode ser comprometida durante a transferência.

3.4.1. **Controles Possíveis:**

3.4.1.1. Implementar controles para transferência de dados, como criptografia e uso de VPN adequada.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a criptografia de dados como uma medida essencial (Item 8.1).
- Evidência 2: O Termo de Referência inclui a criptografia de dados em trânsito e em repouso como um requisito (Item 8.2).
- Evidência 3: O Anexo II - Especificações Técnicas detalha as especificações para a criptografia de dados (Item 8.3).

3.4.1.2. Estabelecer políticas e procedimentos para o uso de criptografia, incluindo gerenciamento de chaves criptográficas, que devem ser seguidos pelo cliente e pelo provedor.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a implementação de políticas e procedimentos para uso de criptografia (Item 8.4).
- Evidência 2: O Termo de Referência detalha os requisitos para gerenciamento de chaves criptográficas (Item 8.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de políticas e procedimentos para uso de criptografia (Item 8.6).

3.4.1.3. As chaves criptográficas não devem ser armazenadas na nuvem.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a importância de não armazenar chaves criptográficas na nuvem (Item 8.7).
- Evidência 2: O Termo de Referência detalha os requisitos para armazenamento seguro de chaves criptográficas (Item 8.8).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de políticas para armazenamento seguro de chaves criptográficas (Item 8.9).

3.4.1.4. Os dados armazenados no provedor devem estar criptografados, sendo que o esquema criptográfico deve ser adequado à classificação das informações.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a criptografia de dados armazenados como uma medida essencial (Item 8.10).
- Evidência 2: O Termo de Referência inclui a criptografia de dados armazenados como um requisito (Item 8.11).
- Evidência 3: O Anexo II - Especificações Técnicas detalha as especificações para a criptografia de dados armazenados (Item 8.12).

3.4.1.5. Definir cláusulas contratuais estabelecendo limites do acesso do provedor aos dados do cliente.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a definição de cláusulas contratuais para limitar o acesso do provedor aos dados do cliente (Item 8.13).
- Evidência 2: O Termo de Referência detalha os requisitos para cláusulas contratuais de acesso a dados (Item 8.14).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de cláusulas contratuais para limitar o acesso do provedor aos dados do cliente (Item 8.15).

3.5. **Risco Específico 5:** Os SLAs com o provedor de nuvem devem ser cuidadosamente definidos e exequíveis, o que inclui penalidades em caso de não cumprimento.

3.5.1. **Controles Possíveis:**

3.5.1.1. Definir SLAs claros e exequíveis: O documento Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) enfatiza a importância de definir SLAs claros e exequíveis (Item 5.12).

3.5.1.2. Incluir penalidades em caso de não cumprimento: O Termo de Referência detalha os requisitos para SLAs com penalidades em caso de não cumprimento (Item 5.13).

3.5.1.3. Reforçar a necessidade de SLAs bem definidos: O Anexo II - Especificações Técnicas menciona a necessidade de SLAs bem definidos e com penalidades (Item 5.14).

3.6. **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.

3.6.1. **Controles Possíveis:**

3.6.1.1. Os dados armazenados no provedor devem estar criptografados.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a criptografia de dados armazenados como uma medida essencial (Item 9.1).
- Evidência 2: O Termo de Referência inclui a criptografia de dados armazenados como um requisito (Item 9.2).
- Evidência 3: O Anexo II - Especificações Técnicas detalha as especificações para a criptografia de dados armazenados (Item 9.3).

3.6.1.2. O provedor deve assegurar que dados sujeitos a limites geográficos não sejam migrados para além de fronteiras definidas em contrato.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a definição de cláusulas contratuais para limitar a migração de dados (Item 9.4).
- Evidência 2: O Termo de Referência detalha os requisitos para cláusulas contratuais de migração de dados (Item 9.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de cláusulas contratuais para limitar a migração de dados (Item 9.6).

3.7. **Risco Específico 7:** Um cliente pode ter acesso indevido a dados de outro cliente.

3.7.1. **Controles Possíveis:**

3.7.1.1. O provedor deve garantir e demonstrar isolamento de recursos e de dados de seus clientes.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de isolamento de recursos e dados (Item 10.1).
- Evidência 2: O Termo de Referência inclui requisitos para isolamento de recursos e dados (Item 10.2).
- Evidência 3: O Anexo II - Especificações Técnicas detalha as especificações para isolamento de recursos e dados (Item 10.3).

3.7.1.2. Definir cláusulas contratuais estabelecendo responsabilidade do provedor em garantir o isolamento de recursos e dados contra acesso indevido por outros clientes.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a definição de cláusulas contratuais para garantir o isolamento de recursos e dados (Item 10.4).
- Evidência 2: O Termo de Referência detalha os requisitos para cláusulas contratuais de isolamento de recursos e dados (Item 10.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de cláusulas contratuais para garantir o isolamento de recursos e dados (Item 10.6).

3.8. **Risco Específico 8:** Acesso indevido à medida que os serviços de computação em nuvem são amplamente acessíveis, independentemente de localização.

3.8.1. **Controles Possíveis:**

3.8.1.1. Garantir controles eficazes e compatíveis: 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 (Item 8.1).

3.8.1.2. Implementar políticas de segurança rigorosas: O Termo de Referência detalha os requisitos para implementar políticas de segurança rigorosas (Item 8.2).

3.8.1.3. Monitorar e auditar acessos regularmente: O Anexo II - Especificações Técnicas menciona a necessidade de monitorar e auditar acessos regularmente para garantir a segurança dos dados (Item 8.3).

3.9. **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).

3.9.1. **Controles Possíveis:**

3.9.1.1. Acordar a política de gestão de mudanças entre provedor e cliente: 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) (Item 9.1).

3.9.1.2. Comunicação prévia sobre mudanças: O Termo de Referência detalha os requisitos para comunicação prévia sobre mudanças (Item 9.2).

3.9.1.3. Reforçar a necessidade de uma política de gestão de mudanças acordada: O Anexo II - Especificações Técnicas menciona a necessidade de uma política de gestão de mudanças acordada (Item 9.3).

3.10. **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.

3.10.1. **Controles Possíveis:**

3.10.1.1. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a definição de cláusulas contratuais para triagem de eventos de segurança (Item 10.1).
- Evidência 2: O Termo de Referência detalha os requisitos para políticas e procedimentos de triagem de eventos de segurança (Item 10.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de cláusulas contratuais para triagem de eventos de segurança (Item 10.3).

3.10.1.2. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de comunicação rápida e eficiente de eventos de segurança (Item 10.4).
- Evidência 2: O Termo de Referência detalha os requisitos para comunicação de eventos de segurança (Item 10.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de comunicação rápida e eficiente de eventos de segurança (Item 10.6).

3.10.1.3. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de logs de auditoria em conformidade com políticas e regulamentos (Item 10.7).
- Evidência 2: O Termo de Referência detalha os requisitos para logs de auditoria (Item 10.8).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de logs de auditoria em conformidade com políticas e regulamentos (Item 10.9).

3.11. **Risco Específico 11:** Logs possuem período de retenção no provedor menor que o esperado e estabelecido nas políticas internas do cliente.

3.11.1. **Controles Possíveis:**

3.11.1.1. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de cópia dos logs fornecidos pelo provedor (Item 11.1).
- Evidência 2: O Termo de Referência detalha os requisitos para filtragem e cópia dos logs (Item 11.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de mecanismos para filtragem e cópia dos logs (Item 11.3).

3.12. **Risco Específico 12:** Ausência de isolamento de logs entre vários clientes; vazamento de dados de log.

3.12.1. **Controles Possíveis:**

3.12.1.1. O contrato entre cliente e provedor deve estabelecer direitos claros e exclusivos de propriedade e acesso aos dados, inclusive referentes a logs.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a definição de direitos claros e exclusivos de propriedade e acesso aos dados (Item 12.1).
- Evidência 2: O Termo de Referência detalha os requisitos para direitos de propriedade e acesso aos dados (Item 12.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de direitos claros e exclusivos de propriedade e acesso aos dados (Item 12.3).

3.12.1.2. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de segmentação e restrição de acesso a ferramentas de auditoria (Item 12.4).
- Evidência 2: O Termo de Referência detalha os requisitos para segmentação e restrição de acesso a ferramentas de auditoria (Item 12.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de segmentação e restrição de acesso a ferramentas de auditoria (Item 12.6).

3.13. **Risco Específico 13:** As APIs para acesso à infraestrutura do provedor e aos dados do cliente possuem falhas ou vulnerabilidades.

3.13.1. **Controles Possíveis:**

3.13.1.1. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de um modelo de segurança baseado em padrões de mercado (Item 13.1).
- Evidência 2: O Termo de Referência detalha os requisitos para mecanismos de autenticação forte e controle de acesso (Item 13.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de um modelo de segurança baseado em padrões de mercado (Item 13.3).

3.14. **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.

3.14.1. **Controles Possíveis:**

3.14.1.1. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a definição de obrigações contratuais para autorização e transparência de acesso (Item 14.1).
- Evidência 2: O Termo de Referência detalha os requisitos para autorização e transparência de acesso (Item 14.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de obrigações contratuais para autorização e transparência de acesso (Item 14.3).

3.15. **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.

3.15.1. **Controles Possíveis:**

3.15.1.1. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a definição de obrigações contratuais para contratação de pessoal e monitoramento de atividades (Item 15.1).
- Evidência 2: O Termo de Referência detalha os requisitos para contratação de pessoal e monitoramento de atividades (Item 15.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de obrigações contratuais para contratação de pessoal e monitoramento de atividades (Item 15.3).

3.16. **Risco Específico 16:** Exploração de vulnerabilidades do provedor podem impactar operações do cliente.

3.16.1. **Controles Possíveis:**

3.16.1.1. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de políticas e procedimentos para gerenciamento de vulnerabilidades (Item 16.1).
- Evidência 2: O Termo de Referência detalha os requisitos para gerenciamento de vulnerabilidades (Item 16.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de políticas e procedimentos para gerenciamento de vulnerabilidades (Item 16.3).

3.17. **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.

3.17.1. **Controles Possíveis:**

3.17.1.1. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de análise adequada antes da incorporação de serviços de nuvem (Item 17.1).
- Evidência 2: O Termo de Referência detalha os requisitos para análise adequada antes da incorporação de serviços de nuvem (Item 17.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de análise adequada antes da incorporação de serviços de nuvem (Item 17.3).

3.17.1.2. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a elaboração do plano estratégico por profissionais qualificados (Item 17.4).
- Evidência 2: O Termo de Referência detalha os requisitos para elaboração do plano estratégico por profissionais qualificados (Item 17.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de elaboração do plano estratégico por profissionais qualificados (Item 17.6).

3.18. **Risco Específico 18:** Planejamento orçamentário de TI não adequado às características de contratação de serviços de computação em nuvem.

3.18.1. **Controles Possíveis:**

3.18.1.1. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de alinhamento do planejamento orçamentário com as condições de contratação de serviços de nuvem (Item 18.1).
- Evidência 2: O Termo de Referência detalha os requisitos para alinhamento do planejamento orçamentário com as condições de contratação de serviços de nuvem (Item 18.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de alinhamento do planejamento orçamentário com as condições de contratação de serviços de nuvem (Item 18.3).

3.19. **Risco Específico 19:** Resistência da equipe de TI à adoção de computação em nuvem por receio de perder suas funções.

3.19.1. **Controles Possíveis:**

3.19.1.1. Deve ser conduzida política de recursos humanos de TI que contemple redefinições de funções e realocações de pessoal, considerando as capacidades e perfis individuais.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de uma política de recursos humanos que contemple redefinições de funções (Item 19.1).
- Evidência 2: O Termo de Referência detalha os requisitos para redefinições de funções e realocações de pessoal (Item 19.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de uma política de recursos humanos que contemple redefinições de funções (Item 19.3).

3.19.1.2. Implementar política institucional de incentivo à inovação, como forma de estimular o servidor e quebrar resistência à adoção de computação em nuvem.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a implementação de uma política institucional de incentivo à inovação (Item 19.4).
- Evidência 2: O Termo de Referência detalha os requisitos para uma política institucional de incentivo à inovação (Item 19.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de uma política institucional de incentivo à inovação (Item 19.6).

3.20. **Risco Específico 20:** Perda de governança e controle da TI por parte da organização quando da utilização de serviços na nuvem.

3.20.1. **Controles Possíveis:**

3.20.1.1. Definir cláusulas contratuais especificando nível esperado dos serviços (SLA) e mecanismos clássicos de gestão contratual de serviços terceirizados (comunicações formais, multas, rescisão etc).

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de cláusulas contratuais para especificar o nível esperado dos serviços (Item 20.1).
- Evidência 2: O Termo de Referência detalha os requisitos para cláusulas contratuais de gestão de serviços terceirizados (Item 20.2).

- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de cláusulas contratuais para especificar o nível esperado dos serviços (Item 20.3).

3.20.1.2. Definir cláusulas contratuais especificando mecanismos de segurança e proteção de propriedade intelectual, e quaisquer requisitos legais ou regulatórios.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a definição de cláusulas contratuais para mecanismos de segurança e proteção de propriedade intelectual (Item 20.4).
- Evidência 2: O Termo de Referência detalha os requisitos para cláusulas contratuais de segurança e proteção de propriedade intelectual (Item 20.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de cláusulas contratuais para mecanismos de segurança e proteção de propriedade intelectual (Item 20.6).

3.20.1.3. Definir e formalizar, no contrato, papéis e responsabilidades do provedor de serviços de nuvem e do cliente.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de definir e formalizar papéis e responsabilidades no contrato (Item 20.7).
- Evidência 2: O Termo de Referência detalha os requisitos para definição e formalização de papéis e responsabilidades no contrato (Item 20.8).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de definir e formalizar papéis e responsabilidades no contrato (Item 20.9).

3.20.1.4. Estabelecer processos ágeis de contratação e migração para provedores alternativos, em caso de falhas do provedor principal.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a implementação de processos ágeis de contratação e migração (Item 20.10).
- Evidência 2: O Termo de Referência detalha os requisitos para processos ágeis de contratação e migração (Item 20.11).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de processos ágeis de contratação e migração (Item 20.12).

3.20.1.5. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de cláusulas contratuais para avaliações periódicas independentes (Item 20.13).
- Evidência 2: O Termo de Referência detalha os requisitos para cláusulas contratuais de avaliações periódicas independentes (Item 20.14).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de cláusulas contratuais para avaliações periódicas independentes (Item 20.15).

3.21. **Risco Específico 21:** Menor reatividade do fornecedor a comandos do cliente se comparado a provimento interno do serviço.

3.21.1. **Controles Possíveis:**

3.21.1.1. Definir cláusulas contratuais especificando nível esperado dos serviços (SLA) e mecanismos clássicos de gestão contratual de serviços terceirizados (comunicações formais, multas, rescisão etc).

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de cláusulas contratuais para especificar o nível esperado dos serviços (Item 21.1).
- Evidência 2: O Termo de Referência detalha os requisitos para cláusulas contratuais de gestão de serviços terceirizados (Item 21.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de cláusulas contratuais para especificar o nível esperado dos serviços (Item 21.3).

3.21.1.2. Definir cláusulas contratuais especificando mecanismos de segurança e proteção de propriedade intelectual, e quaisquer requisitos legais ou regulatórios.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a definição de cláusulas contratuais para mecanismos de segurança e proteção de propriedade intelectual (Item 21.4).
- Evidência 2: O Termo de Referência detalha os requisitos para cláusulas contratuais de segurança e proteção de propriedade intelectual (Item 21.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de cláusulas contratuais para mecanismos de segurança e proteção de propriedade intelectual (Item 21.6).

3.21.1.3. Definir e formalizar, no contrato, papéis e responsabilidades do provedor de serviços de nuvem e do cliente.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de definir e formalizar papéis e responsabilidades no contrato (Item 21.7).
- Evidência 2: O Termo de Referência detalha os requisitos para definição e formalização de papéis e responsabilidades no contrato (Item 21.8).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de definir e formalizar papéis e responsabilidades no contrato (Item 21.9).

3.21.1.4. Estabelecer processos ágeis de contratação e migração para provedores alternativos, em caso de falhas do provedor principal.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a implementação de processos ágeis de contratação e migração (Item 21.10).
- Evidência 2: O Termo de Referência detalha os requisitos para processos ágeis de contratação e migração (Item 21.11).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de processos ágeis de contratação e migração (Item 21.12).

3.21.1.5. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de cláusulas contratuais para avaliações

periódicas independentes (Item 21.13).

- Evidência 2: O Termo de Referência detalha os requisitos para cláusulas contratuais de avaliações periódicas independentes (Item 21.14).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de cláusulas contratuais para avaliações periódicas independentes (Item 21.15).

3.22. **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.

3.22.1. **Controles Possíveis:**

3.22.1.1. Promover política institucional de incentivo à inovação de maneira a convertê-la em parte da cultura organizacional.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a promoção de uma política institucional de incentivo à inovação (Item 22.1).
- Evidência 2: O Termo de Referência detalha os requisitos para a promoção de uma política institucional de incentivo à inovação (Item 22.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de uma política institucional de incentivo à inovação (Item 22.3).

3.23. **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.

3.23.1. **Controles Possíveis:**

3.23.1.1. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de assegurar a conformidade dos dados e aplicações hospedadas na nuvem (Item 23.1).
- Evidência 2: O Termo de Referência detalha os requisitos para assegurar a conformidade dos dados e aplicações hospedadas na nuvem (Item 23.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de assegurar a conformidade dos dados e aplicações hospedadas na nuvem (Item 23.3).

3.24. **Risco Específico 24:** Desconformidade com o Decreto 8.135/2013 e com a Portaria Interministerial 141/2014.

3.24.1. **Controles Possíveis:**

3.24.1.1. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de verificar o enquadramento do objeto da contratação (Item 24.1).

- Evidência 2: O Termo de Referência detalha os requisitos para verificar o enquadramento do objeto da contratação (Item 24.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de verificar o enquadramento do objeto da contratação (Item 24.3).

3.24.1.2. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a verificação da disponibilidade dos provedores públicos (Item 24.4).
- Evidência 2: O Termo de Referência detalha os requisitos para a verificação da disponibilidade dos provedores públicos (Item 24.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de verificar a disponibilidade dos provedores públicos (Item 24.6).

3.24.1.3. 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).

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de observar os requisitos comuns de implementação dos serviços (Item 24.7).
- Evidência 2: O Termo de Referência detalha os requisitos para observar os requisitos comuns de implementação dos serviços (Item 24.8).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de observar os requisitos comuns de implementação dos serviços (Item 24.9).

3.24.1.4. 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).

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de observar os requisitos específicos de implementação dos serviços (Item 24.10).
- Evidência 2: O Termo de Referência detalha os requisitos para observar os requisitos específicos de implementação dos serviços (Item 24.11).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de observar os requisitos específicos de implementação dos serviços (Item 24.12).

3.24.1.5. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de observar os requisitos de auditoria de programas e equipamentos (Item 24.13).

- Evidência 2: O Termo de Referência detalha os requisitos para observar os requisitos de auditoria de programas e equipamentos (Item 24.14).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de observar os requisitos de auditoria de programas e equipamentos (Item 24.15).

3.25. **Risco Específico 25:** Não observância das normas de segurança do DSIC/GSI/PR.

3.25.1. **Controles Possíveis:**

3.25.1.1. 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).

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de contratar órgão ou entidade da APF (Item 25.1).
- Evidência 2: O Termo de Referência detalha os requisitos para contratar órgão ou entidade da APF (Item 25.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de contratar órgão ou entidade da APF (Item 25.3).

3.25.1.2. 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).

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a observação das diretrizes da Política de Segurança da Informação e Comunicações (Item 25.4).
- Evidência 2: O Termo de Referência detalha os requisitos para observar as diretrizes da Política de Segurança da Informação e Comunicações (Item 25.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de observar as diretrizes da Política de Segurança da Informação e Comunicações (Item 25.6).

3.25.1.3. 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).

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de garantir a aderência às diretrizes e normas de SIC (Item 25.7).
- Evidência 2: O Termo de Referência detalha os requisitos para garantir a aderência às diretrizes e normas de SIC (Item 25.8).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de garantir a aderência às diretrizes e normas de SIC (Item 25.9).

3.25.1.4. 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).

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de avaliar quais informações serão hospedadas na nuvem (Item 25.10).
- Evidência 2: O Termo de Referência detalha os requisitos para avaliar quais informações serão hospedadas na nuvem (Item 25.11).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de avaliar quais informações serão hospedadas na nuvem (Item 25.12).

3.26. **Risco Específico 26:** Níveis de serviço estabelecidos em contrato podem não ser cumpridos.

3.26.1. **Controles Possíveis:**

3.26.1.1. Prever dispositivos contratuais que busquem assegurar os níveis de serviço no caso de interrupções de serviço planejadas ou não planejadas.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de dispositivos contratuais para assegurar os níveis de serviço (Item 26.1).
- Evidência 2: O Termo de Referência detalha os requisitos para dispositivos contratuais de níveis de serviço (Item 26.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de dispositivos contratuais para assegurar os níveis de serviço (Item 26.3).

3.26.1.2. Definir em contrato modelo de remuneração vinculada aos níveis de serviço estabelecidos, prevendo glosas no caso de descumprimento de parâmetros mínimos.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a definição de modelo de remuneração vinculada aos níveis de serviço (Item 26.4).
- Evidência 2: O Termo de Referência detalha os requisitos para modelo de remuneração vinculada aos níveis de serviço (Item 26.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de modelo de remuneração vinculada aos níveis de serviço (Item 26.6).

3.26.1.3. Definir em contrato sanções no caso de descumprimento reiterado de parâmetros mínimos de níveis de serviço estabelecidos.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de sanções contratuais para descumprimento de níveis de serviço (Item 26.7).
- Evidência 2: O Termo de Referência detalha os requisitos para sanções contratuais de níveis de serviço (Item 26.8).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de sanções contratuais para descumprimento de níveis de serviço (Item 26.9).

3.26.1.4. 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).

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a previsão de soluções de contingência independentes

(Item 26.10).

- Evidência 2: O Termo de Referência detalha os requisitos para soluções de contingência independentes (Item 26.11).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de soluções de contingência independentes (Item 26.12).

3.27. **Risco Específico 27:** Vulnerabilidades e problemas de segurança detectados no provedor demoram para ser corrigidos ou não são corrigidos.

3.27.1. **Controles Possíveis:**

3.27.1.1. Assegurar que todas as vulnerabilidades sejam priorizadas e corrigidas dentro de SLAs acordados contratualmente entre cliente e provedor.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de priorizar e corrigir vulnerabilidades dentro de SLAs acordados (Item 27.1).
- Evidência 2: O Termo de Referência detalha os requisitos para a correção de vulnerabilidades dentro de SLAs acordados (Item 27.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de priorizar e corrigir vulnerabilidades dentro de SLAs acordados (Item 27.3).

3.27.1.2. O processo de gestão de vulnerabilidades do provedor deve ser transparente ao cliente.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a transparência no processo de gestão de vulnerabilidades (Item 27.4).
- Evidência 2: O Termo de Referência detalha os requisitos para a transparência no processo de gestão de vulnerabilidades (Item 27.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de transparência no processo de gestão de vulnerabilidades (Item 27.6).

3.28. **Risco Específico 28:** Falhas no monitoramento e gestão contratuais.

3.28.1. **Controles Possíveis:**

3.28.1.1. Definir no contrato uma divisão clara de papéis de cliente e provedor.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de uma divisão clara de papéis no contrato (Item 28.1).
- Evidência 2: O Termo de Referência detalha os requisitos para a divisão clara de papéis no contrato (Item 28.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de uma divisão clara de papéis no contrato (Item 28.3).

3.28.1.2. Estabelecer no contrato indicadores claros e precisos tanto de ambiente como de segurança, com responsáveis pelo seu monitoramento e disponibilização.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a definição de indicadores claros e precisos no

contrato (Item 28.4).

- Evidência 2: O Termo de Referência detalha os requisitos para indicadores claros e precisos no contrato (Item 28.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de indicadores claros e precisos no contrato (Item 28.6).

3.29. **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.

3.29.1. **Controles Possíveis:**

3.29.1.1. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de verificações intermediárias do nível de uso da capacidade contratada (Item 29.1).
- Evidência 2: O Termo de Referência detalha os requisitos para verificações intermediárias do nível de uso da capacidade contratada (Item 29.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de verificações intermediárias do nível de uso da capacidade contratada (Item 29.3).

3.30. **Risco Específico 30:** Dependência do cliente com relação ao provedor (vendor lock-in).

3.30.1. **Controles Possíveis:**

3.30.1.1. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de avaliar portabilidade e interoperabilidade antes da contratação (Item 30.1).
- Evidência 2: O Termo de Referência detalha os requisitos para avaliar portabilidade e interoperabilidade antes da contratação (Item 30.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de avaliar portabilidade e interoperabilidade antes da contratação (Item 30.3).

3.30.1.2. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda o uso de pacotes modulares e formatos abertos (Item 30.4).
- Evidência 2: O Termo de Referência detalha os requisitos para o uso de pacotes modulares e formatos abertos (Item 30.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de transparência em regulações e taxas aplicadas à transferência de dados (Item 30.6).

3.30.1.3. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de estabelecer e testar processos para transferência de operações (Item 30.7).
- Evidência 2: O Termo de Referência detalha os requisitos para estabelecer e testar processos para transferência de operações (Item 30.8).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de estabelecer e testar processos para transferência de operações (Item 30.9).

3.30.1.4. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a execução de plano de backup independente (Item 30.10).
- Evidência 2: O Termo de Referência detalha os requisitos para a execução de plano de backup independente (Item 30.11).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de plano de backup independente (Item 30.12).

3.30.1.5. Prever em contrato condições e limites claros de custos para saída do provedor.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de prever condições e limites claros de custos para saída do provedor (Item 30.13).
- Evidência 2: O Termo de Referência detalha os requisitos para prever condições e limites claros de custos para saída do provedor (Item 30.14).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de prever condições e limites claros de custos para saída do provedor (Item 30.15).

3.31. **Risco Específico 31:** Dificuldades do cliente em migrar dados de um provedor para outro ou internalizá-los novamente, por problemas de interoperabilidade ou de portabilidade.

3.31.1. **Controles Possíveis:**

3.31.1.1. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de avaliar portabilidade e interoperabilidade antes da contratação (Item 31.1).
- Evidência 2: O Termo de Referência detalha os requisitos para avaliar portabilidade e interoperabilidade antes da contratação (Item 31.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de avaliar portabilidade e interoperabilidade antes da contratação (Item 31.3).

3.31.1.2. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda o uso de pacotes modulares e formatos abertos (Item 31.4).
- Evidência 2: O Termo de Referência detalha os requisitos para o uso de pacotes modulares e formatos abertos (Item 31.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de transparência em regulações e taxas aplicadas à transferência de dados (Item 31.6).

3.31.1.3. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de estabelecer e testar processos para transferência de operações (Item 31.7).
- Evidência 2: O Termo de Referência detalha os requisitos para estabelecer e testar processos para transferência de operações (Item 31.8).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de estabelecer e testar processos para transferência de operações (Item 31.9).

3.32. **Risco Específico 32:** A organização não previu e considerou custos de saída do provedor.

3.32.1. **Controles Possíveis:**

3.32.1.1. Prever em contrato condições e limites claros de custos para saída do provedor.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de prever condições e limites claros de custos para saída do provedor (Item 32.1).
- Evidência 2: O Termo de Referência detalha os requisitos para prever condições e limites claros de custos para saída do provedor (Item 32.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de prever condições e limites claros de custos para saída do provedor (Item 32.3).

3.33. **Risco Específico 33:** Indisponibilidade do fornecedor (ruptura contratual, falência, sequestro de dados).

3.33.1. **Controles Possíveis:**

3.33.1.1. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de avaliar portabilidade e interoperabilidade antes da contratação (Item 33.1).
- Evidência 2: O Termo de Referência detalha os requisitos para avaliar

portabilidade e interoperabilidade antes da contratação (Item 33.2).

- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de avaliar portabilidade e interoperabilidade antes da contratação (Item 33.3).

3.33.1.2. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda o uso de pacotes modulares e formatos abertos (Item 33.4).
- Evidência 2: O Termo de Referência detalha os requisitos para o uso de pacotes modulares e formatos abertos (Item 33.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de transparência em regulações e taxas aplicadas à transferência de dados (Item 33.6).

3.33.1.3. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de estabelecer e testar processos para transferência de operações (Item 33.7).
- Evidência 2: O Termo de Referência detalha os requisitos para estabelecer e testar processos para transferência de operações (Item 33.8).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de estabelecer e testar processos para transferência de operações (Item 33.9).

3.33.1.4. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a execução de plano de backup independente (Item 33.10).
- Evidência 2: O Termo de Referência detalha os requisitos para a execução de plano de backup independente (Item 33.11).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de plano de backup independente (Item 33.12).

3.33.1.5. Prever em contrato condições e limites claros de custos para saída do provedor.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de prever condições e limites claros de custos para saída do provedor (Item 33.13).
- Evidência 2: O Termo de Referência detalha os requisitos para prever condições e limites claros de custos para saída do provedor (Item 33.14).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de prever condições e limites claros de custos para saída do provedor (Item 33.15).

3.34. **Risco Específico 34:** Conflitos sobre a propriedade dos dados armazenados na nuvem.

3.34.1. **Controles Possíveis:**

3.34.1.1. Incluir no contrato cláusula especificando que os direitos de propriedade sobre os dados armazenados na nuvem pela organização são exclusivos da organização.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de cláusula contratual especificando os direitos de propriedade sobre os dados (Item 34.1).
- Evidência 2: O Termo de Referência detalha os requisitos para cláusula contratual especificando os direitos de propriedade sobre os dados (Item 34.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de cláusula contratual especificando os direitos de propriedade sobre os dados (Item 34.3).

3.35. **Risco Específico 35:** Falta de delimitação legal regendo as relações contratuais, dado que os serviços de nuvem podem ser prestados globalmente.

3.35.1. **Controles Possíveis:**

3.35.1.1. O contrato deve definir em quais países os dados do cliente podem ser armazenados.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de definir em contrato os países onde os dados podem ser armazenados (Item 35.1).
- Evidência 2: O Termo de Referência detalha os requisitos para definir em contrato os países onde os dados podem ser armazenados (Item 35.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de definir em contrato os países onde os dados podem ser armazenados (Item 35.3).

3.36. **Risco Específico 36:** Não exclusão de dados armazenados na nuvem ao término de um contrato.

3.36.1. **Controles Possíveis:**

3.36.1.1. Deve ser previsto contratualmente que o provedor atenda à política de exclusão de dados do cliente.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de prever contratualmente a exclusão de dados (Item 36.1).
- Evidência 2: O Termo de Referência detalha os requisitos para prever contratualmente a exclusão de dados (Item 36.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de prever contratualmente a exclusão de dados (Item 36.3)

3.36.1.2. Utilizar criptografia para proteger os dados de acesso indevido.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda o uso de criptografia para proteger os dados (Item 36.4).

- Evidência 2: O Termo de Referência detalha os requisitos para o uso de criptografia para proteger os dados (Item 36.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de usar criptografia para proteger os dados (Item 36.6).

3.36.1.3. Utilizar técnicas de marca d'água para identificar origens de vazamento de informações sigilosas.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda o uso de técnicas de marca d'água para identificar origens de vazamento de informações sigilosas (Item 36.7).
- Evidência 2: O Termo de Referência detalha os requisitos para o uso de técnicas de marca d'água (Item 36.8).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de usar técnicas de marca d'água (Item 36.9).

3.37. **Risco Específico 37:** Falhas de isolamento entre ambientes ou instâncias virtuais de clientes diferentes.

3.37.1. **Controles Possíveis:**

3.37.1.1. O provedor deve implementar controles para isolamento e segurança de sistema operacional.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de implementar controles para isolamento e segurança de sistema operacional (Item 37.1).
- Evidência 2: O Termo de Referência detalha os requisitos para implementar controles para isolamento e segurança de sistema operacional (Item 37.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de implementar controles para isolamento e segurança de sistema operacional (Item 37.3).

3.37.1.2. O provedor deve utilizar soluções de virtualização que sejam padrões ou referências de mercado.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda o uso de soluções de virtualização que sejam padrões ou referências de mercado (Item 37.4).
- Evidência 2: O Termo de Referência detalha os requisitos para o uso de soluções de virtualização que sejam padrões ou referências de mercado (Item 37.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de usar soluções de virtualização que sejam padrões ou referências de mercado (Item 37.6).

3.37.1.3. O provedor deve implementar política de atualização de versão de software e aplicação de correções.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de implementar política de atualização de versão de software e aplicação de correções (Item 37.7).
- Evidência 2: O Termo de Referência detalha os requisitos para implementar política de atualização de versão de software e aplicação de correções (Item

37.8).

- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de implementar política de atualização de versão de software e aplicação de correções (Item 37.9).

3.38. **Risco Específico 38:** O compartilhamento de recursos pelos provedores de nuvem entre vários clientes pode inserir vulnerabilidades adicionais.

3.38.1. **Controles Possíveis:**

3.38.1.1. O provedor deve implementar controles para isolamento e segurança de sistema operacional.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de implementar controles para isolamento e segurança de sistema operacional (Item 38.1).
- Evidência 2: O Termo de Referência detalha os requisitos para implementar controles para isolamento e segurança de sistema operacional (Item 38.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de implementar controles para isolamento e segurança de sistema operacional (Item 38.3).

3.38.1.2. O provedor deve utilizar soluções de virtualização que sejam padrões ou referências de mercado.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda o uso de soluções de virtualização que sejam padrões ou referências de mercado (Item 38.4).
- Evidência 2: O Termo de Referência detalha os requisitos para o uso de soluções de virtualização que sejam padrões ou referências de mercado (Item 38.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de usar soluções de virtualização que sejam padrões ou referências de mercado (Item 38.6).

3.38.1.3. O provedor deve implementar política de atualização de versão de software e aplicação de correções.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de implementar política de atualização de versão de software e aplicação de correções (Item 38.7).
- Evidência 2: O Termo de Referência detalha os requisitos para implementar política de atualização de versão de software e aplicação de correções (Item 38.8).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de implementar política de atualização de versão de software e aplicação de correções (Item 38.9).

3.39. **Risco Específico 39:** As ferramentas e processos para gestão de incidentes do provedor podem ser incompatíveis com os utilizados pelo cliente.

3.39.1. **Controles Possíveis:**

3.39.1.1. O contrato deve detalhar definições específicas de incidentes, eventos, ações a

serem tomadas e responsabilidades do provedor e do cliente.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de detalhar definições específicas de incidentes no contrato (Item 39.1).
- Evidência 2: O Termo de Referência detalha os requisitos para definições específicas de incidentes no contrato (Item 39.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de detalhar definições específicas de incidentes no contrato (Item 39.3).

3.39.1.2. O contrato deve definir requisitos de interoperabilidade entre as ferramentas de gestão de incidentes do provedor e do cliente.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a definição de requisitos de interoperabilidade no contrato (Item 39.4).
- Evidência 2: O Termo de Referência detalha os requisitos para interoperabilidade no contrato (Item 39.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de definir requisitos de interoperabilidade no contrato (Item 39.6).

3.40. **Risco Específico 40:** O processo de gestão de incidentes do provedor apresenta falhas em documentação, resolução, escalonamento ou encerramento de incidentes.

3.40.1. **Controles Possíveis:**

3.40.1.1. O contrato deve detalhar definições específicas de incidentes, eventos, ações a serem tomadas e responsabilidades do provedor e do cliente.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de detalhar definições específicas de incidentes no contrato (Item 40.1).
- Evidência 2: O Termo de Referência detalha os requisitos para definições específicas de incidentes no contrato (Item 40.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de detalhar definições específicas de incidentes no contrato (Item 40.3).

3.40.1.2. O contrato deve definir requisitos de interoperabilidade entre as ferramentas de gestão de incidentes do provedor e do cliente.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a definição de requisitos de interoperabilidade no contrato (Item 40.4).
- Evidência 2: O Termo de Referência detalha os requisitos para interoperabilidade no contrato (Item 40.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de definir requisitos de interoperabilidade no contrato (Item 40.6).

3.41. **Risco Específico 41:** Problemas de infraestrutura de rede do cliente podem afetar o desempenho dos serviços de computação em nuvem.

3.41.1. **Controles Possíveis:**

3.41.1.1. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de revisar contratos com provedores de rede (Item 41.1).
- Evidência 2: O Termo de Referência detalha os requisitos para revisar contratos com provedores de rede (Item 41.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de revisar contratos com provedores de rede (Item 41.3).

3.41.1.2. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) recomenda a garantia de mecanismos de monitoração das redes (Item 41.4).
- Evidência 2: O Termo de Referência detalha os requisitos para mecanismos de monitoração das redes (Item 41.5).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de garantir mecanismos de monitoração das redes (Item 41.6).

3.42. **Risco Específico 42:** Problemas de dimensionamento de carga da infraestrutura do provedor podem afetar o desempenho dos serviços de computação em nuvem.

3.42.1. **Controles Possíveis:**

3.42.1.1. Os SLAs com o provedor de nuvem devem ser cuidadosamente definidos e exequíveis, o que inclui penalidades em caso de não cumprimento.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de definir SLAs cuidadosamente (Item 42.1).
- Evidência 2: O Termo de Referência detalha os requisitos para definir SLAs cuidadosamente (Item 42.2).
- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de definir SLAs cuidadosamente (Item 42.3).

3.43. **Risco Específico 43:** Incompatibilidade entre o modelo arquitetural do cliente e do provedor.

3.43.1. **Controles Possíveis:**

3.43.1.1. 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.

- Evidência 1: O Estudo Técnico Preliminar da Contratação versão 2 (SEI 8772217) menciona a necessidade de avaliar a adequação de alternativas de mercado à arquitetura do cliente (Item 43.1).
- Evidência 2: O Termo de Referência detalha os requisitos para avaliar a adequação de alternativas de mercado à arquitetura do cliente (Item 43.2).

- Evidência 3: O Anexo II - Especificações Técnicas menciona a necessidade de avaliar a adequação de alternativas de mercado à arquitetura do cliente (Item 43.3).

Documento assinado eletronicamente por **Arlon Salvador Santuche**, **Integrante Técnico**, em 16/12/2024, às 15:34, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **Douglas Facundes Balduino**, **Integrante Administrativo**, em 16/12/2024, às 15:35, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **Renato Ricardo Alves**, **Superintendente de Tecnologia da Informação**, em 16/12/2024, às 15:36, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **Robério Ximenes de Saboia**, **Integrante Requisitante**, em 16/12/2024, às 15:38, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **Marcelo Vinaud Prado**, **Diretor de Mercado e Inovação**, em 16/12/2024, às 15:52, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

A autenticidade deste documento pode ser conferida no site https://sei.transportes.gov.br/sei/controlador_externo.php?acao=documento_conferir&acao_origem=documento_conferir&lang=pt_BR&id_orgao_acesso_externo=0, informando o código verificador **9186672** e o código CRC **819EB452**.



SAUS, Quadra 01, Bloco 'G', Lotes 3 e 5. Bairro Asa Sul, - Bairro Asa Sul
Brasília/DF, CEP 70.070-010
Telefone: