



MINISTÉRIO DA ECONOMIA
Secretaria Especial de Desburocratização, Gestão e Governo Digital
Secretaria de Gestão
Central de Compras
Coordenação-Geral de Contratação de Tecnologia da Informação e Comunicação

MAPA DE GERENCIAMENTO DE RISCOS

INTRODUÇÃO

O gerenciamento de riscos permite ações contínuas de planejamento, organização e controle dos recursos relacionados aos riscos que possam comprometer o sucesso do planejamento da contratação, da realização da licitação 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 de cada possível evento identificado, que corresponde à combinação do impacto e de probabilidade de ocorrência da situação, que possa comprometer a efetividade da contratação, bem como o alcance dos resultados pretendidos com a solução de TIC almejada.

Para cada risco identificado, define-se: a probabilidade de ocorrência dos eventos, os possíveis danos e o impacto, caso o risco ocorra. Além disso, são listados 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.

Após a identificação e classificação, deve-se executar uma análise qualitativa e quantitativa dos riscos. A análise qualitativa dos riscos é realizada por meio da classificação escalar da probabilidade (P) e do impacto (I), ou seja, gerasse um Escore de Risco (ER) que é produto da probabilidade pelo impactou (ER = P x I). As tabelas a seguir ajuda a classificar os riscos com base nesses parâmetros:

Tabela 1: Escala qualitativa de classificação da probabilidade do evento. (Fonte: Manual de gestão de riscos do TCU, 2018)

Classificação	Descrição	Valor
Raro	Acontece apenas em situações excepcionais. Não há histórico conhecido do evento ou não há indícios que sinalizem sua ocorrência.	0,10
Pouco provável	O histórico conhecido aponta para baixa frequência de ocorrência no prazo associado ao objetivo	0,30
Provável	Repete-se com frequência razoável no prazo associado ao objetivo ou há indícios que possa ocorrer nesse horizonte	0,50
Muito provável	Repete-se com elevada frequência no prazo associado ao objetivo ou há muitos indícios que ocorrerá nesse horizonte	0,70
Praticamente Certo	Ocorrência quase garantida no prazo associado ao objetivo	0,90

Tabela 2: Escala qualitativa de classificação do impacto do evento. (Fonte: Manual de gestão de riscos do TCU, 2018)

Classificação	Descrição	Valor
Muito Baixo	Compromete minimamente o atingimento do objetivo; para fins práticos, não altera o alcance do objetivo/resultado.	0,05
Baixo	Compromete em alguma medida o alcance do objetivo, mas não impede o alcance da maior parte do objetivo/resultado.	0,10
Moderado	Compromete razoavelmente o alcance do objetivo/resultado.	0,20
Alto	Compromete a maior parte do atingimento do objetivo/resultado.	0,40
Muito Alto	Compromete totalmente ou quase totalmente o atingimento do objetivo/resultado.	0,80

A análise quantitativa dos riscos consiste na classificação conforme o resultado do ER do risco. Tal classificação resultará no nível do risco e direcionará as ações relacionadas aos riscos durante a fase de planejamento e gestão do contrato. A figura a seguir apresenta a Matriz Probabilidade x Impacto, instrumento responsável pela definição dos critérios quantitativos de classificação do nível de risco.



(Fonte: Guia do Conhecimento em Gerenciamento de Projetos - PMBOK®, quinta edição)

O nível de risco é representado pelas cores conforme figura a seguir:

Baixo
Médio
Alto

O produto da probabilidade de ocorrência do evento pelo impacto de cada risco deve se enquadrar em uma região da matriz de riscos. Caso o risco enquadre-se na região verde, seu nível de risco é entendido como baixo, logo admite-se a aceitação ou adoção das medidas preventivas. Se estiver na região amarela, entende-se como médio; e se estiver na região vermelha, entende-se como nível de risco alto. Nos casos de riscos classificados como médio e alto, devem-se adotar obrigatoriamente as medidas preventivas ou fatores de controle a fim de reenquadrar o nível inicial dos riscos identificados como inerentes para que eles possam se tornar riscos residuais. Ou ainda, aceitar os riscos identificados conforme o apetite a risco da instituição.

2 - IDENTIFICAÇÃO E ANÁLISE DOS PRINCIPAIS RISCOS

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
PC01	<i>Questionamentos excessivos no pregão.</i>	Planejamento da Contratação	0,50	0,10	0,05
PC02	<i>Licitação deserta ou com lote deserto.</i>	Planejamento da Contratação	0,30	0,40	0,12
PC03	<i>Rotatividade da equipe do ME.</i>	Planejamento da Contratação	0,30	0,10	0,03
PC04	<i>Contratada se recusar a assinar o contrato.</i>	Planejamento da Contratação	0,10	0,80	0,08
PC05	<i>Incapacidade da empresa vencedora em executar o contrato.</i>	Planejamento da Contratação	0,30	0,40	0,12
PC06	<i>Falência da empresa vencedora.</i>	Planejamento da Contratação	0,30	0,40	0,12
GC01	Indisponibilidade dos serviços.	Gestão Contratual	0,10	0,20	0,02
GC02	Comprometimento da Confidencialidade e Integridade das informações.	Gestão Contratual	0,10	0,80	0,08
GC03	Dependência frente ao provedor (vendor lock-in).	Gestão Contratual	0,50	0,10	0,05
RS01	<i>Modelo sem o devido alinhamento com os órgãos de controle.</i>	Risco da Solução	0,10	0,40	0,04
RS02	<i>Requisitos técnicos amplamente abertos para atender ao maior número de concorrentes em função do princípio da competitividade.</i>	Risco da Solução	0,50	0,05	0,025
RS03	<i>Exposição excessiva a riscos de segurança nos serviços de computação em nuvem.</i>	Risco da Solução	0,30	0,40	0,12
RS04	<i>Perda de parceria entre broker e o provedor de nuvem.</i>	Risco da Solução	0,10	0,40	0,04
RS05	<i>Desistência do provedor de nuvem.</i>	Risco da Solução	0,10	0,40	0,04
RS06	<i>Falha de disponibilidade de dados e/ou sistemas.</i>	Risco da Solução	0,10	0,40	0,04
RS07	<i>Baixa maturidade dos órgãos que utilizarem o contrato no uso dos recursos em nuvem.</i>	Risco da Solução	0,50	0,20	0,10
RS08	<i>Apresentação de Preços inexequíveis.</i>	Risco da Solução	0,30	0,20	0,06
RS09	<i>Quantitativo insuficiente para atender as demandas.</i>	Risco da Solução	0,30	0,40	0,12
RS10	<i>Não aderência ao modelo proposto.</i>	Risco da Solução	0,10	0,40	0,04
RS11	<i>Não obtenção de economia e ganho de escala real com a contratação.</i>	Risco da Solução	0,10	0,20	0,02
RS12	<i>Falhas na Prova de conceito.</i>	Risco da Solução	0,10	0,40	0,04
RS13	<i>Falta de capacidade da empresa em atender os contratos oriundos da Ata.</i>	Risco da Solução	0,10	0,20	0,02
RC01	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.	Risco de controle; Tema: Segurança da informação; Categoria de risco: Indisponibilidade do serviço.	0,30	0,80	0,24
RC02	Indisponibilidade de elementos da infraestrutura do cliente que são críticos para o acesso a serviços na nuvem.	Risco de controle; Tema: Segurança da informação; Categoria de risco: Indisponibilidade do serviço.	0,50	0,40	0,2
RC03	Controle de acesso inexistente ou insuficiente para assegurar a confidencialidade dos dados armazenados na nuvem.	Risco de controle; Tema: Segurança da informação; Categoria de risco: Confidencialidade e integridade de dados.	0,30	0,20	0,06
RC04	A segurança dos dados transmitidos para o provedor de nuvem pela internet pode ser comprometida durante a transferência.	Risco de controle; Tema: Segurança da informação; Categoria de risco: Confidencialidade e integridade de dados.	0,30	0,10	0,03
RC05	Acesso indevido do provedor aos dados.	Risco de controle; Tema: Segurança da informação; Categoria de risco: Confidencialidade e integridade de dados.	0,30	0,20	0,06
RC06	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.	Risco de controle; Tema: Segurança da informação; Categoria de risco: Confidencialidade e integridade de dados.	0,10	0,40	0,04
RC07	Um cliente pode ter acesso indevido a dados de outro cliente.	Risco de controle; Tema: Segurança da informação; Categoria de risco: Confidencialidade e integridade de dados.	0,10	0,40	0,04
RC08	Acesso indevido à medida que os serviços de computação em nuvem são amplamente acessíveis, independentemente de localização.	Risco de controle; Tema: Segurança da informação; Categoria de risco: Confidencialidade e integridade de dados.	0,10	0,40	0,04

RC09	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).	Risco de controle; Tema: Segurança da informação; Categoria de risco: Gestão de mudanças.	0,30	0,20	0,06
RC10	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.	Risco de controle; Tema: Segurança da informação; Categoria de risco: Trilhas de auditoria.	0,10	0,10	0,01
RC11	Logs possuem período de retenção no provedor menor que o esperado e estabelecido nas políticas internas do cliente.	Risco de controle; Tema: Segurança da informação; Categoria de risco: Trilhas de auditoria.	0,10	0,10	0,01
RC12	Ausência de isolamento de logs entre vários clientes; vazamento de dados de log.	Risco de controle; Tema: Segurança da informação; Categoria de risco: Trilhas de auditoria.	0,10	0,20	0,02
RC13	As APIs para acesso à infraestrutura do provedor e aos dados do cliente possuem falhas ou vulnerabilidades.	Risco de controle; Tema: Segurança da informação; Categoria de risco: Segurança de interfaces de programação (APIs).	N/A	N/A	N/A
RC14	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.	Risco de controle; Tema: Segurança da informação; Categoria de risco: Acesso indevido por invasor interno.	0,10	0,10	0,01
RC15	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.	Risco de controle; Tema: Segurança da informação; Categoria de risco: Acesso indevido por invasor interno.	0,10	0,10	0,01
RC16	Exploração de vulnerabilidades do provedor podem impactar operações do cliente.	Risco de controle; Tema: Segurança da informação; Categoria de risco: Atualizações e correções de segurança.	0,10	0,20	0,02
RC17	Dimensionamento inadequado das vantagens e riscos relativos à incorporação de serviços de computação em nuvem em função das características e requisitos individuais da organização.	Risco de controle; Tema: Governança e gestão de riscos; Categoria de risco: Planejamento.	0,30	0,40	0,12
RC18	Planejamento orçamentário de TI não adequado às características de contratação de serviços de computação em nuvem.	Risco de controle; Tema: Governança e gestão de riscos; Categoria de risco: Planejamento.	0,10	0,40	0,04
RC19	Resistência da equipe de TI à adoção de computação em nuvem por receio de perder suas funções.	Risco de controle; Tema: Governança e gestão de riscos; Categoria de risco: Política de recursos humanos.	0,10	0,40	0,04
RC20	Perda de governança e controle da TI por parte da organização quando da utilização de serviços na nuvem.	Risco de controle; Tema: Governança e gestão de riscos; Categoria de risco: Governança.	0,30	0,40	0,12
RC21	Menor reatividade do fornecedor a comandos do cliente se comparado a provimento interno do serviço.	Risco de controle; Tema: Governança e gestão de riscos; Categoria de risco: Governança.	0,30	0,20	0,06
RC22	Falta de apoio interno devido à cultura organizacional e percepção do cliente de que há maiores riscos associados a serviços em nuvem.	Risco de controle; Tema: Governança e gestão de riscos; Categoria de risco: Governança.	0,30	0,40	0,12
RC23	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.	Risco de controle; Tema: Governança e gestão de riscos; Categoria de risco: Legislação e normativos pertinentes	0,10	0,40	0,04
RC24	Desconformidade com o Decreto 8.135/2013 e com a Portaria Interministerial 141/2014.	Risco de controle; Tema: Governança e gestão de riscos; Categoria de risco: Legislação e normativos pertinentes	0,10	0,40	0,04
RC25	Não observância das normas de segurança do DSIC/GSI/PR.	Risco de controle; Tema: Governança e gestão de riscos; Categoria de risco: Legislação e normativos pertinentes.	0,10	0,40	0,04
RC26	Níveis de serviço estabelecidos em contrato podem não ser cumpridos.	Risco de controle; Tema: Contratação e gestão contratual; Categoria de risco: Gestão contratual.	0,30	0,40	0,12
RC27	Vulnerabilidades e problemas de segurança detectados no provedor demoram para ser corrigidos ou não são corrigidos.	Risco de controle; Tema: Contratação e gestão contratual; Categoria de risco: Gestão contratual.	0,30	0,40	0,12
RC28	Falhas no monitoramento e gestão contratuais.	Risco de controle; Tema: Contratação e gestão contratual;	0,30	0,20	0,06

		Categoria de risco: Gestão contratual.			
RC29	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.	Risco de controle; Tema: Contratação e gestão contratual; Categoria de risco: Gestão contratual.	0,50	0,40	0,2
RC30	Dependência do cliente com relação ao provedor (vendedor lock-in).	Risco de controle; Tema: Contratação e gestão contratual; Categoria de risco: Dependência frente ao provedor.	0,30	0,40	0,12
RC31	Dificuldades do cliente em migrar dados de um provedor para outro ou internalizá-los novamente, por problemas de interoperabilidade ou de portabilidade.	Risco de controle; Tema: Contratação e gestão contratual; Categoria de risco: Dependência frente ao provedor.	0,30	0,40	0,12
RC32	A organização não previu e considerou custos de saída do provedor.	Risco de controle; Tema: Contratação e gestão contratual; Categoria de risco: Dependência frente ao provedor.	0,30	0,40	0,12
RC33	Indisponibilidade do fornecedor (ruptura contratual, falência, sequestro de dados).	Risco de controle; Tema: Contratação e gestão contratual; Categoria de risco: Dependência frente ao provedor.	0,30	0,40	0,12
RC34	Conflitos sobre a propriedade dos dados armazenados na nuvem.	Risco de controle; Tema: Contratação e gestão contratual; Categoria de risco: Falhas contratuais.	0,30	0,40	0,12
RC35	Falta de delimitação legal regendo as relações contratuais, dado que os serviços de nuvem podem ser prestados globalmente.	Risco de controle; Tema: Contratação e gestão contratual; Categoria de risco: Falhas contratuais.	0,30	0,40	0,12
RC36	Não exclusão de dados armazenados na nuvem ao término de um contrato.	Risco de controle; Tema: Contratação e gestão contratual; Categoria de risco: Falhas contratuais.	0,30	0,05	0,015
RC37	Falhas de isolamento entre ambientes ou instâncias virtuais de clientes diferentes.	Risco de controle; Tema: Infraestrutura de TI; Categoria de risco: Falhas relativas à infraestrutura de TI.	0,30	0,40	0,12
RC38	O compartilhamento de recursos pelos provedores de nuvem entre vários clientes pode inserir vulnerabilidades adicionais	Risco de controle; Tema: Infraestrutura de TI; Categoria de risco: Falhas relativas à infraestrutura de TI.	0,30	0,40	0,12
RC39	As ferramentas e processos para gestão de incidentes do provedor podem ser incompatíveis com os utilizados pelo cliente.	Risco de controle; Tema: Infraestrutura de TI; Categoria de risco: Falhas relativas à infraestrutura de TI.	0,30	0,20	0,06
RC40	O processo de gestão de incidentes do provedor apresenta falhas em documentação, resolução, escalonamento ou encerramento de incidentes.	Risco de controle; Tema: Infraestrutura de TI; Categoria de risco: Falhas relativas à infraestrutura de TI.	0,30	0,20	0,06
RC41	Problemas de infraestrutura de rede do cliente podem afetar o desempenho dos serviços de computação em nuvem.	Risco de controle; Tema: Infraestrutura de TI; Categoria de risco: Falhas relativas à infraestrutura de TI.	0,50	0,20	0,1
RC42	Problemas de dimensionamento de carga da infraestrutura do provedor podem afetar o desempenho dos serviços de computação em nuvem.	Risco de controle; Tema: Infraestrutura de TI; Categoria de risco: Falhas relativas à infraestrutura de TI.	0,30	0,40	0,12
RC43	Incompatibilidade entre o modelo arquitetural do cliente e do provedor.	Risco de controle; Tema: Infraestrutura de TI; Categoria de risco: Falhas relativas à infraestrutura de TI.	0,30	0,40	0,12

Legenda: P – Probabilidade; I – Impacto.
1 A qual natureza o risco está associado: fases do Processo da Contratação ou Solução Tecnológica.
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).

3 - AVALIAÇÃO E TRATAMENTO DOS RISCOS IDENTIFICADOS

Nesta seção todos os riscos identificados são analisados (compreende-se a natureza do risco e identifica-se o nível de risco) e avaliados quanto a melhor ação a ser tomada para diminuir seus impactos, quais sejam: evitar, reduzir ou mitigar, transferir ou compartilhar, e aceitar ou tolerar o risco. Os quadros a seguir apresentam a análise e avaliação de cada risco identificado.

RISCO PC01	
Risco:	Questionamentos excessivos no pregão.

Probabilidade:	Provável
Impacto:	Baixo
Nível de Risco:	Baixo
Dano 1:	Legitimidade de pregão colocada em questão.
Tratamento:	Mitigar.

Id	Ação Preventiva	Responsável
1	Definir as regras gerais da contratação de forma clara no Edital e em seus anexos, atentar à legislação vigente no tocante a exigências de marcas, modelos e requisitos excludentes.	Equipe de Planejamento da Contratação
2	Elaborar documento com itens passíveis de impugnação com suas respectivas respostas.	Equipe de Planejamento da Contratação
3	Realizar consulta pública para validar o modelo de contratação.	Equipe de Planejamento da Contratação
Id	Ação de Contingência	Responsável
1	Republicação do Edital com correção dos itens alvos de impugnação.	Área de Contratos

RISCO PC02	
Risco:	Licitação deserta ou com lote deserto.
Probabilidade:	Pouco provável
Impacto:	Alto
Nível de Risco:	Médio
Dano 1:	Não realizar a licitação tendo que republicar o edital e abrir novo prazo para a realização do pregão.
Tratamento:	Mitigar.

Id	Ação Preventiva	Responsável
1	Encaminhar termo de referência durante a fase de cotação de preços para a maior quantidade de possíveis interessados em participar da licitação.	Equipe de Planejamento da Contratação
2	Distribuir, caso seja possível, o quantitativo de serviços existentes em lotes que atendam ao interesse do Governo e percentualmente sejam atrativos.	Equipe de Planejamento da Contratação
3	Avisar, assim que publicado o edital em DOU, às empresas que encaminharam propostas comerciais da data de realização do pregão.	Órgão Gerenciador
Id	Ação de Contingência	Responsável
1	Republicação do Edital observando requisitos que poderiam ter provocado a desistência de possíveis empresas interessadas.	Órgão Gerenciador, Equipe de Planejamento da Contratação e CONJUR

RISCO PC03	
Risco:	Rotatividade da equipe do MP
Probabilidade:	Pouco provável
Impacto:	Baixo
Nível de Risco:	Baixo
Dano 1:	Dificuldade para realização do Planejamento da Contratação e confecção dos artefatos exigidos pela IN4/2014.
Tratamento:	Mitigar.

Id	Ação Preventiva	Responsável
1	Formalizar a necessidade de servidores efetivos lotados formalmente nas áreas demandante, técnica e administrativa.	Equipe de Planejamento da Contratação
Id	Ação de Contingência	Responsável
1	Comunicar os impactos à alta gestão.	Integrantes Requisitante e Técnico

RISCO PC04	
Risco:	Contratada se recusar a assinar o contrato.
Probabilidade:	Raro
Impacto:	Muito alto
Nível de Risco:	Médio
Dano 1:	Não concluir a licitação tendo que republicar o edital e abrir novo prazo para a realização do pregão.
Tratamento:	Mitigar.

Id	Ação Preventiva	Responsável
1	Definir punição no edital para empresa adjudicada que não assinar o contrato dentro do prazo estipulado.	Órgão Contratante
Id	Ação de Contingência	Responsável
1	Adjudicar novo fornecedor ou promover nova contratação.	Órgão Contratante

RISCO PC05	
Risco:	Incapacidade da empresa vencedora em executar o contrato.
Probabilidade:	Pouco provável
Impacto:	Alto
Nível de Risco:	Médio
Dano 1:	Atraso nos serviços
Tratamento:	Mitigar.

Id	Ação Preventiva	Responsável
1	Incluir no Edital níveis mínimos de serviços, sanções e os requisitos de qualidade que sejam condizentes com a importância dos serviços a serem prestados.	Integrantes requisitante e técnico
2	Colocar regra no Edital que, em caso de inexecução parcial ou total do contrato, a segunda colocada poderá ser habilitada.	Equipe de Planejamento da Contratação
3	Exigir documentação comprovatória que a licitante já prestou serviços semelhante ao contratado.	Equipe de Planejamento da Contratação
4	Exigir o nível máximo de garantia contratual permitido em lei com vistas a assegurar o compromisso da empresa na prestação adequada dos serviços.	Equipe de Planejamento da Contratação
Id	Ação de Contingência	Responsável
1	Fiscalização do contrato com aplicação de sanções previstas quando ocorrer alguma falha contratual e, em último caso, cancelar contrato e adjudicar novo fornecedor ou promover nova contratação.	Gestor do Contrato

RISCO PC06	
Risco:	Falência da empresa vencedora.
Probabilidade:	Pouco provável
Impacto:	Alto
Nível de Risco:	Médio
Dano 1:	Atraso nos serviços
Tratamento:	Mitigar.

Id	Ação Preventiva	Responsável
1	Exigir requisitos habilitatórios relativos à qualificação econômica – financeira.	Equipe de Planejamento da Contratação
2	Exigir garantia contratual, conforme Art. 56 da Lei 8.666/93.	Equipe de Planejamento da Contratação
Id	Ação de Contingência	Responsável
1	Adjudicar novo fornecedor ou promover nova contratação.	Órgão Gerenciador

RISCO GC01	
Risco:	Indisponibilidade dos Serviços.
Probabilidade:	Raro
Impacto:	Moderado
Nível de Risco:	Baixo
Dano 1:	Não atendimento dos objetivos da contratação. Serviços indisponíveis causando prejuízo ao usuário e a administração.
Tratamento:	Mitigar.

Id	Ação Preventiva	Responsável
1	Estabelecer requisitos que garantam que a CONTRATADA possui condições de garantir a disponibilidade dos serviços, a exemplo da exigência de que os provedores de nuvem possuam certificação ISO 27018 e 27017.	Equipe de Planejamento da Contratação
2	Estabelecer níveis de serviços elevados para o tempo de disponibilidade da solução.	Fiscais Requisitante e Técnico
Id	Ação de Contingência	Responsável
1	Realizar a migração de serviços para outro ambiente (interno ou outra nuvem).	Gestor do Contrato

RISCO GC02	
Risco:	Comprometimento da Confidencialidade e Integridade das informações.
Probabilidade:	Raro
Impacto:	Muito alto
Nível de Risco:	Médio
Dano 1:	Dados do Ministério serem expostos ou corrompidos.
Tratamento:	Mitigar

Id	Ação Preventiva	Responsável
1	Especificar no Termo de Referência requisitos que prevejam a criação de acesso somente autorizado aos sistemas.	Integrantes Requisitante e Técnico
2	Definir que os dados e aplicações deverão ser mantidos em datacenters instalados fisicamente no país.	Equipe de Planejamento da Contratação
3	Definir que o foro para qualquer assunto relativo ao contrato será o Brasileiro.	Equipe de Planejamento da Contratação
4	Observância e implementação das recomendações da NC14/DSIC.	Integrantes Requisitante e Técnico
5	Definir Centro de Custos para fins de isolar as aplicações em nuvem do Ministério.	Equipe de Planejamento da Contratação
6	Prever serviços de conexão direto ao centro de dados dos provedores e previsão de utilização de certificados SSL.	Integrantes Requisitante e Técnico
Id	Ação de Contingência	Responsável
1	Garantir que a execução das ordens de serviço seja acompanhada por profissionais qualificados e, caso não seja cumprido, aplicar as punições cabíveis.	Órgão Contratante

RISCO GC03	
Risco:	Dependência frente ao provedor (vendor lock-in).
Probabilidade:	Provável
Impacto:	Baixo
Nível de Risco:	Baixo
Dano 1:	Inviabilidade de migração contratual para outro provedor decorrente da dependência.
Dano 2:	
Tratamento:	Mitigar.

Id	Ação Preventiva	Responsável
1	Estabelecer processo de avaliação do tipo de informação a ser migrada para o ambiente de nuvem conforme processo proposto pela NC14/DSIC.	Equipe de Planejamento da Contratação
2	Definir arquitetura de aplicações passíveis de serem migradas para outros provedores.	Integrantes Requisitante e Técnico
Id	Ação de Contingência	Responsável
1	Negociação entre as áreas envolvidas.	Gestor do Contrato

RISCOS DA SOLUÇÃO							
Tipo	Descrição Risco	Causa	Consequência	Probabilidade (P)	Impacto (I)	Nível de Risco (P x I)	Ação
Imagem	RS01 Modelo sem o devido alinhamento com os órgãos de controle	Urgência e criticidade	Adiamento da realização do certame	0,10	0,40	0,04	1. Observação de Acórdãos que tratem do assunto; 2. Realização de reuniões com os órgãos de controle para análise de riscos; 3. Compartilhar minuta do TR para sugestões e críticas
Estratégico	RS02 Requisitos técnicos amplamente abertos para atender ao maior número de concorrentes em função do princípio da competitividade	Baixa exigência de requisitos técnicos	Empresa contratada sem qualificação técnica suficiente para prestar serviço desse porte	15 alto	15 alto	0,025	1. Análise criteriosa das especificações técnicas para o atendimento dos objetivos da contratação; 2. Alinhamento das exigências de capacidade técnica da empresa a ser contratada; 3. Análise dos atestados de capacidade técnica e, se necessária, realização de diligências para comprovação da prestação satisfatória dos serviços.

Estratégico	RS03 Exposição excessiva a riscos de segurança nos serviços de computação em nuvem	Falta de exigência de qualificação técnica em segurança de nuvem	Baixa qualidade da empresa contratada Eventual incidente de segurança da informação	0,30	0,40	0,12	Alterar o edital para exigir a apresentação explícita da certificação da empresa quanto à aderência/cumprimento da norma de serviços em nuvem ABNT NBR ISO/IEC 27017:2016 e da 27018:2016
Estratégico	RS04 Perda de parceria entre broker e o provedor de nuvem	estratégia comercial volátil, forte dependência da empresa contratada com o provedor de nuvem	Interrupção contratual	0,10	0,40	0,04	Exigir que o broker assegure a manutenção do contrato com o provedor
Estratégico	RS05 Desistência do provedor de nuvem	estratégia comercial volátil	Interrupção contratual	0,10	0,40	0,04	definir obrigações para o broker efetuar a migração em caso de troca de provedor que independa da decisão da contratante.
Estratégico	RS06 Falha de disponibilidade de dados e/ou sistemas	Não exigência de pelo menos dois datacenters no Brasil	Indisponibilidade de serviços em execução e perda de informações em caso de acidentes	0,10	0,40	0,04	Exigir que o broker contrate um provedor que possua plano de continuidade, recuperação de desastres e contingência de negócio, que possa ser testado regularmente, objetivando a disponibilidade dos dados e serviços em caso de interrupção, bem como desenvolver e colocar em prática procedimentos de respostas a incidentes relacionados com os serviços.
Estratégico	RS07 Baixa maturidade dos órgãos que utilizarem o contrato no uso dos recursos em nuvem	serviço novo, em especial no governo; falta de capacitação específica.	Subutilização do contrato, mal aproveitamento das funcionalidades oferecidas pelo contrato	0,50	0,20	0,10	formar corpo técnico com conhecimento em demandar e gerenciar contratos de nuvem
Estratégico	RS08 Apresentação de Preços inexequíveis	conta do MP, referência da esplanada	Licitacao fracassada	0,30	0,20	0,06	solicitar e validar planilha de custo da empresa
Imagem	RS09 Quantitativo insuficiente para atender as demandas	falha no levantamento dos quantitativos, novos projetos	Não execução de projetos importantes para a Adm. Pública	0,30	0,40	0,12	utilizar saldo das adesões, limitar o uso do quantitativo por órgãos e realizar nova licitação
Estratégico	RS10 Não aderência ao modelo proposto	modelo inovador	Interrupção contratual	0,10	0,40	0,04	validar a proposta com o mercado e especialista da área
Estratégico	RS11 Não obtenção de economia e ganho de escala real com a contratação.	Fornecedores superfaturar os preços	Maior custo para a APF	0,10	0,20	0,02	Manter planilha de preços com pesquisa atualizada
Estratégico	RS12 Falhas na	roteiro de testes simples	Licitação fracassada	0,10	0,40	0,04	implantar o modelo já utilizado pelo TCU

	<i>Prova de conceito</i>						
Imagem	RS13 <i>Falta de capacidade da empresa em atender os contratos oriundos da Ata</i>	<i>dificuldade em atender vários contratos simultâneos</i>	<i>Interrupção contratual</i>	0,10	0,20	0,02	<i>avaliar o quantitativo de cada órgão antes da assinatura do contrato</i>

RISCOS DE CONTROLE

A tabela a seguir apresenta a relação de riscos de controle mapeados pelo Tribunal de Contas da União em sede do Acórdão 1.793/2015 - Plenário e as respectivas ações previstas pelo ME para mitigá-los.

TEMA: SEGURANÇA DA INFORMAÇÃO			
CATEGORIA DE RISCO: INDISPONIBILIDADE DO SERVIÇO			
RISCO ESPECÍFICO			
RC01- 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.		Probabilidade (P) 0,30	Impacto (I) 0,80 Nível de Risco (PxI) 0,24
CONTROLES POSSÍVEIS		CRITÉRIOS	
O plano de continuidade de negócio deve considerar as partes do negócio que estão na nuvem e levar em consideração tanto as características do negócio como do provedor.		As salvaguardas e controles necessários à garantia da continuidade da infraestrutura do provedor forma implementadas por meio dos seguintes pontos: a. Exigência do PCN do provedor: item 3.1.6 - o provedor que integra a solução deve possuir, plano de continuidade, recuperação de desastres e contingência de negócio, que possa ser testado regularmente, objetivando a disponibilidade dos dados e serviços em caso de interrupção, bem como desenvolver e colocar em prática procedimentos de respostas a incidentes relacionados com os serviços. b. Exigência de capacidade mínima: item 3.1.7, a Solução deverá dispor de sistema de hardware e dados para missão crítica com política de “Disaster Recovery”, balanceamento, conectividade e backup/restore durante toda a vigência do contrato a garantia de Recovery Time Objective (RTO) em até 3 horas e de Recovery Point Objective (RPO) de 1 hora. c. Solicitado Nível Mínimo de Serviço de 99.741% (item 9.3.2.2) de acordo com a necessidade e criticidade das informações passíveis de serem migradas para nuvem. d. Foi considerada a possibilidade de transferência dos dados principais para a estrutura interna temporariamente nos itens 2.1.23.27 e 3.1.15.	
Considerar capacidade do provedor de trabalhar com multirregiões no provedor e poder transferir carga de uma região para outra.			
O plano de continuidade de negócio para nuvem pode considerar mais de um provedor como contingência.			
Considerar a alternativa de utilizar sua própria infraestrutura de TI como contingência.			
OS SLAs com o provedor de nuvem devem ser cuidadosamente definidos e exequíveis, o que inclui penalidades em caso de não cumprimento.		Solicitado SLA de 99.741%. item 9.3.2.2	
RISCO ESPECÍFICO			
RC02 - Indisponibilidade de elementos da infraestrutura do cliente que são críticos para o acesso a serviços na nuvem		Probabilidade (P) 0,50	Impacto (I) 0,40 Nível de Risco (PxI) 0,2
CONTROLES POSSÍVEIS		CRITÉRIOS	
Deve ser definido e documentado um método para determinar o impacto de qualquer indisponibilidade à organização, incluindo de serviços que estão na nuvem a dependência dos elementos da infraestrutura do órgão que são necessários à utilização dos mesmos, que deverá, também, estabelecer prioridades para recuperação e período máximo tolerável para a indisponibilidade.		Previsto de forma abrangente. item 3.1.6 O provedor que integra a solução deve possuir, plano de continuidade, recuperação de desastres e contingência de negócio, que possa ser testado regularmente, objetivando a disponibilidade dos dados e serviços em caso de interrupção, bem como desenvolver e colocar em prática procedimentos de respostas a incidentes relacionados com os serviços.	
CATEGORIA DE RISCO: CONFIDENCIALIDADE E INTEGRIDADE DE DADOS			
RISCO ESPECÍFICO			

RC03 - Controle de acesso inexistente ou insuficiente para assegurar a confidencialidade dos dados armazenados na nuvem		Probabilidade (P) 0,30	Impacto (I) 0,20	Nível de Risco (PxI) 0,06
CONTROLES POSSÍVEIS		CRITÉRIOS		
Os dados devem ser submetidos à classificação prévia da informação, antes de serem transmitidos para a nuvem		Processo do ME que poderá ser observado pelos demais órgãos que aderirem ao serviço objeto desta contratação. Deve ser previsto no diagnóstico dos projetos através de atividade que permita relacionamento com os gestores da informação.		
Implementar controle de acesso lógico apropriado ao grau de confidencialidade dos dados armazenados na nuvem		Processo do ME que poderá ser observado pelos demais órgãos que aderirem ao serviço objeto desta contratação. Já realizado atualmente.		
RISCO ESPECÍFICO				
RC04 - A segurança dos dados transmitidos para o provedor de nuvem pela internet pode ser comprometida durante a transferência		Probabilidade (P) 0,30	Impacto (I) 0,10	Nível de Risco (PxI) 0,03
CONTROLES POSSÍVEIS		CRITÉRIOS		
Implementar controles para transferência de dados, como criptografia e uso de VPN adequada		Itens 21 e 22 da Tabela 1 - USN		
RISCO ESPECÍFICO				
RC05 - Acesso indevido do provedor aos dados		Probabilidade (P) 0,30	Impacto (I) 0,20	Nível de Risco (PxI) 0,06
CONTROLES POSSÍVEIS		CRITÉRIOS		
Estabelecer políticas e procedimentos para o uso de criptografia, incluindo gerenciamento de chaves criptográficas, que devem ser seguidos pelo cliente e pelo provedor		Será previsto no edital: A solução deve dispor de mecanismo para gestão integrada de chaves de segurança que permita tratar, gerenciar e proteger chaves usando várias camadas de segurança;		
As chaves criptográficas não devem ser armazenadas na nuvem		A solução deve permitir que dados criptografados, chaves de criptografia e chaves mestras sejam armazenadas e protegidas em hosts separados e protegidos por várias camadas de proteção		
Os dados armazenados no provedor devem estar criptografados, sendo que o esquema criptográfico deve ser adequado à classificação das informações		Deve ser observado a NC 14 em relação ao tipo de informação a ser disponibilizada na nuvem		
Definir cláusulas contratuais estabelecendo limites do acesso do provedor aos dados do cliente		Exigir que será vedada a CONTRATADA ou ao provedor acesso aos dados hospedados na infraestrutura de nuvem, sem prévia e formal autorização por parte da CONTRATANTE;		
RISCO ESPECÍFICO				
RC06 - 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		Probabilidade (P) 0,10	Impacto (I) 0,40	Nível de Risco (PxI) 0,04
CONTROLES POSSÍVEIS		CRITÉRIOS		
Os dados armazenados no provedor devem estar criptografados		Criptografia está prevista no TR, porém em casos de dados públicos não trataremos com criptografia.		
O provedor deve assegurar que dados sujeitos a limites geográficos não sejam migrados para além de fronteiras definidas em contrato.		Vide: 6.7.7. Da Segurança dos Dados e Informações		
RISCO ESPECÍFICO				
RC07 - Um cliente pode ter acesso indevido a dados de outro cliente.		Probabilidade (P) 0,10	Impacto (I) 0,40	Nível de Risco (PxI) 0,04
CONTROLES POSSÍVEIS		CRITÉRIOS		

O provedor deve garantir e demonstrar isolamento de recursos e de dados de seus clientes	Item 6.7.7.7.		
Definir cláusulas contratuais estabelecendo responsabilidade do provedor em garantir o isolamento de recursos e dados contra acesso indevido por outros clientes	Item 3.1.19		
RISCO ESPECÍFICO			
RC08 - Acesso indevido à medida que os serviços de computação em nuvem são amplamente acessíveis, independentemente de localização.	Probabilidade (P) 0,10	Impacto (I) 0,40	Nível de Risco (PxI) 0,04
CONTROLES POSSÍVEIS	CRITÉRIOS		
O provedor deve garantir controles eficazes e compatíveis com as políticas e procedimentos do cliente para gerenciamento de identidades de usuários e controle de acessos.	Previsto através da Certificações de Segurança. Item 3.1.16 Item 3 – Requisitos de Segurança		
CATEGORIA DE RISCO: GESTÃO DE MUDANÇAS			
RISCO ESPECÍFICO			
RC09 - 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).	Probabilidade (P) 0,30	Impacto (I) 0,20	Nível de Risco (PxI) 0,06
CONTROLES POSSÍVEIS	CRITÉRIOS		
A política para gestão de mudanças deve ser acordada entre provedor e cliente, e este último deve ser comunicado com antecedência sobre mudanças (por exemplo, utilizando processos do ITIL).	Será adotado o processo de gestão de mudanças do ME que poderá ser utilizado pelos demais órgãos.		
CATEGORIA DE RISCO: TRILHAS DE AUDITORIA			
RISCO ESPECÍFICO			
RC10 - 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	Probabilidade (P) 0,10	Impacto (I) 0,10	Nível de Risco (PxI) 0,01
CONTROLES POSSÍVEIS	CRITÉRIOS		
Cláusulas contratuais devem definir políticas e procedimentos que devem ser estabelecidos para triagem dos eventos relacionados à segurança e garantir o gerenciamento de incidentes completo e ágil	Previsto através da Certificações de Segurança. Item 3.1.16 Previsto através através de logs de segurança de todas as atividades Item 3.1.17 Através do serviço técnico especializado para a implantação de Logs previstos no item 2.2.18.33		
Eventos de segurança de informação devem ser comunicados através de canais predefinidos de comunicação, de maneira rápida e eficiente, e de acordo com os requisitos legais, regulatórios e contratuais			
Logs de auditoria do provedor que registram atividades de acesso de usuários privilegiados, tentativas de acesso autorizados e não autorizados, exceções do sistema, e eventos de segurança da informação devem ser mantidos em conformidade com as políticas e regulamentos aplicáveis, e devem estar de acordo com as políticas do cliente			
RISCO ESPECÍFICO			
RC11 - Logs possuem período de retenção no provedor menor que o esperado e estabelecido nas políticas internas do cliente	Probabilidade (P) 0,10	Impacto (I) 0,10	Nível de Risco (PxI) 0,01
CONTROLES POSSÍVEIS	CRITÉRIOS		
O cliente deve prever cópia dos logs fornecidos pelo provedor, de acordo com sua própria política de retenção; deve haver, da parte do provedor, um mecanismo para	Previsto através através de logs de segurança de todas as atividades Item 3.1.17 e Item 2.1.10		

filtragem e cópia dos logs gerados pelo fornecedor para a área do cliente			
RISCO ESPECÍFICO			
RC12 - Ausência de isolamento de logs entre vários clientes; vazamento de dados de log	Probabilidade (P) 0,10	Impacto (I) 0,20	Nível de Risco (PxI) 0,02
CONTROLES POSSÍVEIS	CRITÉRIOS		
O contrato entre cliente e provedor deve estabelecer direitos claros e exclusivos de propriedade e acesso aos dados, inclusive referentes a logs	Item 3.1.12		
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	Item 3.1.18		
CATEGORIA DE RISCO: SEGURANÇA DE INTERFACES DE PROGRAMAÇÃO (APIs)			
RISCO ESPECÍFICO			
RC13 - As APIs para acesso à infraestrutura do provedor e aos dados do cliente possuem falhas ou vulnerabilidades	Probabilidade (P) N/A	Impacto (I) N/A	Nível de Risco (PxI) N/A
CONTROLES POSSÍVEIS	CRITÉRIOS		
O modelo de segurança das interfaces do provedor deve ser desenvolvido com base em padrões de mercado, incluindo mecanismos de autenticação forte de usuários e controle de acesso para restringir o acesso aos dados do cliente	Não se aplica, pois não estamos solicitando SaaS.		
CATEGORIA DE RISCO: ACESSO INDEVIDO POR INVASOR INTERNO			
RISCO ESPECÍFICO			
RC14 - 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	Probabilidade (P) 0,10	Impacto (I) 0,10	Nível de Risco (PxI) 0,01
CONTROLES POSSÍVEIS	CRITÉRIOS		
Definir no contrato as obrigações do provedor quanto a requisitos mínimos de autorização e transparência de acesso do provedor aos ativos físicos e virtuais do cliente, bem como a respeito da necessidade de divulgação ao cliente de suas políticas e orientações específicas	Previsto através da Certificações de Segurança 27017 e 27018.		
RISCO ESPECÍFICO			
RC15 - 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	Probabilidade (P) 0,10	Impacto (I) 0,10	Nível de Risco (PxI) 0,01
CONTROLES POSSÍVEIS	CRITÉRIOS		
Definir no contrato as obrigações do provedor quanto a requisitos mínimos de contratação de pessoal e de monitoramento de suas atividades, bem como a respeito da necessidade de divulgação ao cliente de suas políticas e orientações específicas	Exigir a contratação de pessoal qualificado.		
CATEGORIA DE RISCO: ATUALIZAÇÕES E CORREÇÕES DE SEGURANÇA			
RISCO ESPECÍFICO			
RC16 - Exploração de vulnerabilidades do provedor podem impactar operações do cliente	Probabilidade (P) 0,10	Impacto (I) 0,20	Nível de Risco (PxI) 0,02

Controles possíveis	Critérios		
Políticas, procedimentos e mecanismos devem ser estabelecidos e implementados pelo provedor para gerenciamento de vulnerabilidades conhecidas e atualizações de software, garantindo que aplicações, sistemas e vulnerabilidades de dispositivos de rede sejam avaliadas, e que atualizações de segurança fornecidas sejam aplicadas em tempo hábil, priorizando os patches mais críticos	Previsto no Edital – Item 3 – Requisitos de Segurança.		
TEMA: GOVERNANÇA E GESTÃO DE RISCOS			
CATEGORIA DE RISCO: PLANEJAMENTO			
RISCO ESPECÍFICO			
RC17 - Dimensionamento inadequado das vantagens e riscos relativos à incorporação de serviços de computação em nuvem em função das características e requisitos individuais da organização	Probabilidade (P) 0,30	Impacto (I) 0,40	Nível de Risco (PxI) 0,12
CONTROLES POSSÍVEIS	CRITÉRIOS		
A incorporação de computação em nuvem ao plano estratégico de TI deve ser precedida de análise adequada de modo a assegurar que serviços de nuvem são a solução mais apropriada para as necessidades da organização.	Deverá estar previsto no PDTIC.		
A incorporação de computação em nuvem ao plano estratégico de TI deve ser elaborada por um time de profissionais qualificados de TI e de negócio, e todas as partes interessadas na organização devem ser consultadas.			
RISCO ESPECÍFICO			
RC18 - Planejamento orçamentário de TI não adequado às características de contratação de serviços de computação em nuvem.	Probabilidade (P) 0,10	Impacto (I) 0,40	Nível de Risco (PxI) 0,04
CONTROLES POSSÍVEIS	CRITÉRIOS		
O planejamento orçamentário deve estar alinhado com as condições de contratação de serviços de computação em nuvem, particularmente quanto à transformação de verba de investimento na compra de equipamentos de TIC para verba de custeio dos serviços de nuvem	O planejamento orçamentário foi revisto para inclusão das despesas previstas na modalidade em nuvem.		
CATEGORIA DE RISCO: POLÍTICA DE RECURSOS HUMANOS			
RISCOS ESPECÍFICOS			
RC19 - Resistência da equipe de TI à adoção de computação em nuvem por receio de perder suas funções	Probabilidade (P) 0,10	Impacto (I) 0,40	Nível de Risco (PxI) 0,04
CONTROLES POSSÍVEIS	CRITÉRIOS		
Deve ser conduzida política de recursos humanos de TI que contemple redefinições de funções e realocações de pessoal, considerando as capacidades e perfis individuais	O ME já possui experiência em Nuvem, logo este risco é baixo. Entretanto, a análise dos estudos técnicos preliminares de órgãos entrantes deverá possibilitar a seleção daqueles órgãos que possuem baixo risco na utilização de recursos em nuvem.		
Implementar política institucional de incentivo à inovação, como forma de estimular o servidor e quebrar resistência à adoção de computação em nuvem			
CATEGORIA DE RISCO: GOVERNANÇA			
RISCOS ESPECÍFICOS			
RC20 - Perda de governança e controle da TI por parte da organização quando da utilização de serviços na nuvem	Probabilidade (P) 0,30	Impacto (I) 0,40	Nível de Risco (PxI) 0,12

RC21 - Menor reatividade do fornecedor a comandos do cliente se comparado a provimento interno do serviço		Probabilidade (P) 0,30	Impacto (I) 0,20	Nível de Risco (PxI) 0,06
CONTROLES POSSÍVEIS		CRITÉRIOS		
Definir cláusulas contratuais especificando nível esperado dos serviços (SLA) e mecanismos clássicos de gestão contratual de serviços terceirizados (comunicações formais, multas, rescisão etc)		Item 9.3		
Definir cláusulas contratuais especificando mecanismos de segurança e proteção de propriedade intelectual, e quaisquer requisitos legais ou regulatórios		Item 6.2.22		
Definir e formalizar, no contrato, papéis e responsabilidades do provedor de serviços de nuvem e do cliente		Conforme descrito no Item 6		
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		Previsto através da Certificações de Segurança. Item 3.1.16 – Vigência das Certificações		
RISCO ESPECÍFICO				
RC22 - Falta de apoio interno devido à cultura organizacional e percepção do cliente de que há maiores riscos associados a serviços em nuvem		Probabilidade (P) 0,30	Impacto (I) 0,40	Nível de Risco (PxI) 0,12
CONTROLES POSSÍVEIS		CRITÉRIOS		
Promover política institucional de incentivo à inovação de maneira a convertê-la em parte da cultura organizacional		O escopo dos serviços a serem migrados para a nuvem considerou aqueles serviços com baixo impacto em relação à mudança cultural.		
CATEGORIA DE RISCO: LEGISLAÇÃO E NORMATIVOS PERTINENTES				
RISCO ESPECÍFICO				
RC23 - 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		Probabilidade (P) 0,10	Impacto (I) 0,40	Nível de Risco (PxI) 0,04
CONTROLES POSSÍVEIS		CRITÉRIOS		
A organização deve ser capaz de assegurar a conformidade dos dados e aplicações hospedadas na nuvem com os requisitos de padrões, legais e regulatórios, aos quais o negócio está sujeito, de maneira contínua e atualizada		Contratação conforme IN-04, Portaria-STI nº 20, de 2016 e NC-GSI nº 14/2018.		
RISCO ESPECÍFICO				
RC24 - Desconformidade com o Decreto 8.135/2013 e com a Portaria Interministerial 141/2014		Probabilidade (P) 0,10	Impacto (I) 0,40	Nível de Risco (PxI) 0,04
Controles possíveis		Critérios		
Verificar, na fase de planejamento da contratação, se o objeto da contratação pode ser enquadrado como "comunicação de dados da APF", conforme a Portaria Interministerial 141/2014, art. 1º e art. 11		Foi realizado consulta pública às empresas públicas em relação a esta iniciativa e a resposta orientou a condução do processo.		
Até o término da fase de planejamento da contratação, verificar se a contratação deve ser feita por meio de provedor público ou privado, consultando a disponibilidade dos provedores públicos de atender às especificações técnicas e níveis de serviço do objeto da contratação, conforme a Portaria Interministerial 141/2014, art. 5º, § 3º				

Especialmente no caso de contratação de fornecedor privado, observar os requisitos comuns de implementação dos serviços estabelecidos pela Portaria Interministerial 141/2014: padrões do e-Ping (art. 8º) e obrigações que deverão estar contidas no termo de referência ou projeto básico e no contrato (art. 9º)				
Especialmente no caso de contratação de fornecedor privado, observar os requisitos específicos de implementação dos serviços estabelecidos pela Portaria Interministerial 141/2014: requisitos mínimos para serviços de redes de telecomunicações (art. 10) e critérios mínimos de segurança da informação (art. 12)				
Especialmente no caso de contratação de fornecedor privado, observar os requisitos de auditoria de programas e equipamentos estabelecidos pela Portaria Interministerial 141/2014 (arts. 13 e 14), os quais deverão estar previstos no termo de referência ou projeto básico e no contrato				
Risco específico				
RC25 - Não observância das normas de segurança do DSIC/GSI/PR		Probabilidade (P) 0,10	Impacto (I) 0,40	Nível de Risco (PxI) 0,04
Controles possíveis		Critérios		
No caso de infraestrutura de nuvem para sistemas estruturantes da APF, contratar órgão ou entidade da APF (item 4.2.3 da Norma Complementar 19/IN01 /DSIC/GSIPR)		Considerou-se a observância integral da NC 14		
Antes de adotar a tecnologia de computação em nuvem, observar as diretrizes da sua Política de Segurança da Informação e Comunicações (SIC), do seu processo de Gestão de Riscos de SIC e do seu processo de Gestão de Continuidade de Negócios nos aspectos relacionados à SIC (item 5.1 da Norma Complementar 14/IN01 /DSIC/GSIPR)				
Ao contratar ou implementar um serviço de computação em nuvem, garantir que o ambiente, incluindo infraestrutura e canal de comunicação, esteja aderente às diretrizes e normas de SIC do GSI/PR, que a legislação brasileira prevaleça e que o contrato de prestação de serviço contenha cláusulas de segurança quanto às informações hospedadas na nuvem (item 5.2 da Norma Complementar 14/IN01/DSIC/GSIPR)				
Avaliar quais informações serão hospedadas na nuvem, considerando o processo de classificação da informação, o valor do ativo de informação, os controles de acesso físicos e lógicos, o modelo de serviço e de implementação de computação em nuvem e a localização geográfica onde as informações serão armazenadas (item 5.3 da Norma Complementar 14/IN01/DSIC/GSIPR)				
Tema: Contratação e gestão contratual				
Categoria de risco: Gestão contratual				
Risco específico				
RC26 - Níveis de serviço estabelecidos em contrato podem não ser cumpridos		Probabilidade (P) 0,30	Impacto (I) 0,40	Nível de Risco (PxI) 0,12
Controles possíveis		Critérios		
Prever dispositivos contratuais que busquem assegurar os níveis de serviço no caso de interrupções de serviço planejadas ou não planejadas		Item 9.3.5.a 9.4.21 – Sanções Administrativas e procedimentos para glosa no pagamento Gestão de capacidade do ambiente de rede interno ao ME. Aquisições de		

Definir em contrato modelo de remuneração vinculada aos níveis de serviço estabelecidos, prevendo glosas no caso de descumprimento de parâmetros mínimos		laminas Blade e equipamentos Nutanix para crescimento do ambiente e possível recepção dos ambientes principais da Nuvem, em caso de descontinuidade do serviço. Item 3.1.8 A CONTRATANTE a qualquer tempo poderá solicitar a realização de simulação de portabilidade das aplicações hospedadas na Nuvem para a rede interna do ME e este serviço será contratado através de UST's previstos neste Edital.		
Definir em contrato sanções no caso de descumprimento reiterado de parâmetros mínimos de níveis de serviço estabelecidos				
Prever soluções de contingência independentes de provedor específico (portabilidade do serviço para outro fornecedor, contrato de contingência em caso de falha do fornecedor principal, espelhamento do serviço em infraestrutura própria etc)				
Risco específico				
RC27 - Vulnerabilidades e problemas de segurança detectados no provedor demoram para ser corrigidos ou não são corrigidos		Probabilidade (P)	Impacto (I)	Nível de Risco (PxI)
		0,30	0,40	0,12
Controles possíveis		Critérios		
Assegurar que todas as vulnerabilidades sejam priorizadas e corrigidas dentro de SLAs acordados contratualmente entre cliente e provedor		Previsto através da Certificações de Segurança. Item 3.1.16 Item 3 – Requisitos de Segurança		
O processo de gestão de vulnerabilidades do provedor deve ser transparente ao cliente				
Risco específico				
RC28 - Falhas no monitoramento e gestão contratuais		Probabilidade (P)	Impacto (I)	Nível de Risco (PxI)
		0,30	0,20	0,06
Controles possíveis		Critérios		
Definir no contrato uma divisão clara de papéis de cliente e provedor		Item 6 Deveres e responsabilidades		
Estabelecer no contrato indicadores claros e precisos tanto de ambiente como de segurança, com responsáveis pelo seu monitoramento e disponibilização				
Risco específico				
RC29 - 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		Probabilidade (P)	Impacto (I)	Nível de Risco (PxI)
		0,50	0,40	0,2
Controles possíveis		Critérios		
Prever verificações intermediárias do nível de uso da capacidade contratada, alertas quando atingidos patamares de recursos e tetos de recursos máximos utilizáveis em função do orçamento disponível		Tecnicamente teremos um painel que representa o andamento dos custos da Nuvem conforme item 2.1.10		
Categoria de risco: Dependência frente ao provedor				
Riscos específicos				
RC30 - Dependência do cliente com relação ao provedor (vendedor lock-in)		Probabilidade (P)	Impacto (I)	Nível de Risco (PxI)
		0,30	0,40	0,12
RC31 - Dificuldades do cliente em migrar dados de um provedor para outro ou internalizá-los novamente, por problemas de interoperabilidade ou de portabilidade		Probabilidade (P)	Impacto (I)	Nível de Risco (PxI)
		0,30	0,40	0,12

RC32 - A organização não previu e considerou custos de saída do provedor		Probabilidade (P) 0,30	Impacto (I) 0,40	Nível de Risco (PxI) 0,12
RC33 - Indisponibilidade do fornecedor (ruptura contratual, falência, sequestro de dados)		Probabilidade (P) 0,30	Impacto (I) 0,40	Nível de Risco (PxI) 0,12
Controles possíveis	Critérios			
Os requisitos da organização para portabilidade e interoperabilidade devem ser cuidadosamente avaliados antes da contratação de nuvem frente às alternativas disponíveis no mercado, a fim de mitigar relações de dependência com o provedor	Itens 2.1.22.3, 3.1.8, 7.7.2, 7.7.4, 2.2.18.21, 2.2.18.24, 2.1.8, 2.1.21.2 e 2.2.11.5 Anexo V			
estabelecidos e testados, de maneira a viabilizar a transferência de operações de um provedor de computação em nuvem para outro provedor alternativo				
Especialmente no caso de informações críticas para o negócio, convém considerar a execução de plano de backup independente do fornecedor, duplicando dados em intervalos periódicos				
Prever em contrato condições e limites claros de custos para saída do provedor				
Categoria de risco: Falhas contratuais				
Risco específico				
RC34 - Conflitos sobre a propriedade dos dados armazenados na nuvem		Probabilidade (P) 0,30	Impacto (I) 0,40	Nível de Risco (PxI) 0,12
Controles possíveis	Critérios			
Incluir no contrato cláusula especificando que os direitos de propriedade sobre os dados armazenados na nuvem pela organização são exclusivos da organização	Itens 2.1.11.3, 2.1.19, 3.1.22, 6.2.22, 7.7.10 e 9.3.12.			
Risco específico				
RC35 - Falta de delimitação legal regendo as relações contratuais, dado que os serviços de nuvem podem ser prestados globalmente		Probabilidade (P) 0,30	Impacto (I) 0,40	Nível de Risco (PxI) 0,12
Controles possíveis	Critérios			
O contrato deve definir em quais países os dados do cliente podem ser armazenados	Itens 2.1.8 e 3.1.16.			
Risco específico				
RC36 - Não exclusão de dados armazenados na nuvem ao término de um contrato		Probabilidade (P) 0,30	Impacto (I) 0,05	Nível de Risco (PxI) 0,015
Controles possíveis	Critérios			
Deve ser previsto contratualmente que o provedor atenda à política de exclusão de dados do cliente	Itens 3.1.14, 3.1.15, 3.3.2, 3.4.2, 3.4.5, 3.4.6, 3.4.7, 3.4.8, 3.1.13			
Utilizar criptografia para proteger os dados de acesso indevido				
Utilizar técnicas de marca d'água para identificar origens				

de vazamento de informações sigilosas			
Tema: Infraestrutura de TI			
Categoria de risco: Falhas relativas à infraestrutura de TI			
Riscos específicos			
RC37 - Falhas de isolamento entre ambientes ou instâncias virtuais de clientes diferentes	Probabilidade (P) 0,30	Impacto (I) 0,40	Nível de Risco (PxI) 0,12
RC38 - O compartilhamento de recursos pelos provedores de nuvem entre vários clientes pode inserir vulnerabilidades adicionais	Probabilidade (P) 0,30	Impacto (I) 0,40	Nível de Risco (PxI) 0,12
Controles possíveis	Critérios		
O provedor deve implementar controles para isolamento e segurança de sistema operacional	Item 3.1.19, 3.1.20, 3.1.21 e 3.1.24		
O provedor deve utilizar soluções de virtualização que sejam padrões ou referências de mercado			
O provedor deve implementar política de atualização de versão de software e aplicação de correções			
Riscos específicos			
RC39 - As ferramentas e processos para gestão de incidentes do provedor podem ser incompatíveis com os utilizados pelo cliente	Probabilidade (P) 0,30	Impacto (I) 0,20	Nível de Risco (PxI) 0,06
RC40 - O processo de gestão de incidentes do provedor apresenta falhas em documentação, resolução, escalonamento ou encerramento de incidentes	Probabilidade (P) 0,30	Impacto (I) 0,20	Nível de Risco (PxI) 0,06
Controles possíveis	Critérios		
O contrato deve detalhar definições específicas de incidentes, eventos, ações a serem tomadas e responsabilidades do provedor e do cliente	Item 3.1.4, 3.1.6 e 3.1.10		
O contrato deve definir requisitos de interoperabilidade entre as ferramentas de gestão de incidentes do provedor e do cliente			
Risco específico			
RC41 - Problemas de infraestrutura de rede do cliente podem afetar o desempenho dos serviços de computação em nuvem	Probabilidade (P) 0,50	Impacto (I) 0,20	Nível de Risco (PxI) 0,1
Controles possíveis	Critérios		
Deve-se buscar garantir que os mecanismos de monitoração das redes consigam distinguir entre problemas internos, na rede dos provedores, ou fora do seu escopo			
Risco específico			
RC42 - Problemas de dimensionamento de carga da infraestrutura do provedor podem afetar o desempenho dos serviços de computação em nuvem	Probabilidade (P) 0,30	Impacto (I) 0,40	Nível de Risco (PxI) 0,12
Controles possíveis	Critérios		

OS SLA's com o provedor de nuvem devem ser cuidadosamente definidos e exequíveis, o que inclui penalidades em caso de não cumprimento		Os insumos serão providos pelos serviços de monitoramento. Itens 3.1.5 e 2.2.11.2		
Risco específico				
RC43 - Incompatibilidade entre o modelo arquitetural do cliente e do provedor		Probabilidade (P) 0,30	Impacto (I) 0,40	Nível de Risco (PxI) 0,12
Controles possíveis		Critérios		
O estudo de viabilidade técnica (estudos técnicos preliminares) da contratação deve avaliar se alternativas de mercado e soluções disponíveis adequam-se à arquitetura do cliente, ou se a adaptação da arquitetura do cliente à do provedor é viável		Realizado no ETP da Contratação		

5 - APROVAÇÃO E ASSINATURA

Conforme § 5º do art. 38 da IN SGD/ME nº 1, de 2019, o Mapa de Gerenciamento de Riscos deve ser assinado pela Equipe de Planejamento da Contratação, nas fases de Planejamento da Contratação e de Seleção de Fornecedores, e pela Equipe de Fiscalização do Contrato, na fase de Gestão do Contrato. A Equipe de Planejamento da Contratação foi instituída pelo Documento de Oficialização da Demanda nº 6086856, de 26 de fevereiro de 2020.

CRISTIANO POUBEL DE CASTRO

Integrante Requisitante

Documento assinado eletronicamente

JÚLIO CÉSAR PROENÇA

Integrante Técnico

Documento assinado eletronicamente

THAIS CABRAL DE MELLO

Integrante Técnico

Documento assinado eletronicamente

GILNARA PINTO PEREIRA

Integrante Administrativo

Documento assinado eletronicamente

ABDIAS DA SILVA OLIVEIRA

Integrante Administrativo



Documento assinado eletronicamente por **Cristiano Jorge Poubel de Castro, Analista em Tecnologia da Informação**, em 24/10/2020, às 11:25, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Júlio César Proença, Analista em Tecnologia da Informação**, em 26/10/2020, às 07:45, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Thais Cabral de Mello, Analista em Tecnologia da Informação**, em 26/10/2020, às 07:57, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Abdias da Silva Oliveira, Analista**, em 26/10/2020, às 09:44, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Gilnara Pinto Pereira, Analista**, em 26/10/2020, às 09:49, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site http://sei.fazenda.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **11157619** e o código CRC **361A6628**.

Referência: Processo nº 19973.100103/2020-51.

SEI nº 11157619