FUNDAÇÃO NACIONAL DE SAÚDE

MAPA DE RISCOS

PROCESSO Nº 25100.011868/2019-56

1. INTRODUÇÃO

1.1. O objetivo deste documento é consolidar informações sobre a análise de riscos referente a aquisição de licenças de solução de gateway de segurança de e-mails (AntiSpam) para a FUNASA, com fornecimento de serviço de instalação e configuração, suporte, manutenção especializada e garantia de toda a solução por 12 (doze) meses, e ainda treinamento.

2. ESTRATÉGIA DE GERENCIAMENTO DE RISCOS

2.1. O gerenciamento de riscos no âmbito deste trabalho está alinhado com os princípios e diretrizes expostos em publicações, normas e padrões internacionais, como o padrão ISO 31000:2009 (Gerenciamento de Risco – Princípios e diretrizes) e o guia ISO 73:2009 (Gerenciamento de Risco - Vocabulário), ambos publicados pela Organização Internacional para Padronização (ISO), e a Norma para Gerenciamento de Risco, da Federação Europeia das Associações de Gerenciamento de Risco.

2.2. No contexto desse documento, risco é definido como a combinação da probabilidade de um acontecimento e das suas consequências. O gerenciamento de riscos compreende o conjunto de atividades relacionadas à identificação, análise e planejamento de ações a serem executadas em resposta aos riscos identificados, compreendendo a criação de estratégias para a potencialização dos resultados de eventos positivos e a minimização das consequências de eventos negativos.

2.3. A análise de riscos constante neste documento inicialmente visa a identificação e o tratamento de riscos sob uma perspectiva qualitativa, tendo em vista a sua relevância e oportunidade para o sucesso da execução de serviços de TI por parte da CGMTI. Por se tratar de um processo dinâmico, a análise de riscos será atualizada à medida que novas informações relevantes forem identificadas e registradas. Sempre que possível, as informações quantitativas referentes aos riscos identificados também devem ser incorporadas ao processo.

2.4. O escopo dessa análise de riscos abrange a gestão do respectivo contrato. Assim, essa análise de riscos se destina a subsidiar os gestores de contratos.

2.5. Para cada risco identificado, deve-se proceder a sua descrição, estimar a probabilidade de ocorrência e o seu grau de impacto, bem como definir as estratégias para tratamento dos riscos, de modo a evitar, mitigar, transferir ou aceitar os efeitos dos riscos do tipo ameaça (negativos) e potencializar os efeitos dos riscos do tipo oportunidade (positivos).

2.6. No modelo de categorização proposto os riscos são agrupados em três zonas: verde, amarela e vermelha. Na zona verde se encontram os riscos com valores de 1, 2 ou 3, na amarela, os riscos de valores 4 ou 6, e na zona vermelha os riscos com valor 9. Esse agrupamento é útil para indicar a antecedência com que as ações identificadas para tratamento dos riscos devem ser adotadas. Assim, na zona verde o risco é considerado mínimo (remoto) e as ações são levadas a cabo somente se o risco de fato se concretizar. Na zona amarela o risco é moderado (possível) e deve-se considerar a adoção de medidas para minimizá-lo. Por fim, na zona vermelha o risco é alto (provável) e devem ser adotadas medidas para tratar o risco antes que ele ocorra. No modelo em comento a atribuição de valores para os elementos que compõem o risco e o seu agrupamento numa zona de risco é relativamente simples, mas o que é realmente importante e essencial é a ampla compreensão dos riscos e a forma como eles serão gerenciados.

2.7. Por fim, o gerenciamento de riscos envolve o monitoramento dos riscos identificados e a execução de ações para o seu devido tratamento. O monitoramento deve ocorrer enquanto o risco for considerado significativo ou até que seja concluído o escopo de trabalho no qual o risco se encontra mapeado. Quanto ao tratamento de riscos, são definidos quatro tipos de ações de resposta aos riscos:

- eliminar a possibilidade do risco se materializar ou neutralizar suas consequências;
- diminuir a possibilidade do risco se materializar ou minimizar suas consequências;
- transferir/repassar a um terceiro as consequências negativas e a responsabilidade pelo tratamento do risco; ou
- aceitar/assumir as consequências da concretização do risco.

2.8. Nas seções seguintes deste documento são identificados e analisados os riscos, sendo apresentadas estratégias e ações para o seu devido tratamento. O mapeamento realizado teve como base o “Guia de boas práticas em contratação de soluções de tecnologia da informação - riscos e controles para o planejamento da contratação” (versão 1.0), elaborado pelo Tribunal de Contas da União, sendo adaptado à realidade da área de TI da Funasa. Além disso, o gerenciamento de riscos objeto deste documento incorpora diversas ações de controle propostas no âmbito dos processos estabelecidos no COBIT (*Control Objectives for Information and related Technology*), versão 5.0, desenvolvido pela *Information Systems Audit and Control Association* – ISACA.

3. IDENTIFICAÇÃO DE RISCOS

3.1. A fim de facilitar a compreensão de todos os aspectos que compõem esta análise de riscos, são apresentadas na tabela 1 informações gerais que visam à identificação de riscos propriamente, restando outros itens que compõem as respectivas análises e estratégias de tratamento para as seções seguintes.

3.2. Os riscos foram agrupados por fases do processo de contratação das soluções de TI. Dessa forma, os riscos são identificados por códigos com formato “RF-XX”, onde “R” representa “risco”, “F” assume o valor “P”, “E” ou “G”, indicando que o risco se refere, respectivamente, à fase de Planejamento da contratação, Execução de contratos celebrados ou Geral (tanto planejamento quanto execução), e “XX” é uma sequência numérica do tipo “01”, “02”, etc, usada para identificar unicamente o risco no grupo no qual se enquadra. Por fim, na tabela de identificação de riscos também estão descritos alguns aspectos aos quais os riscos se referem.

TABELA 1. IDENTIFICAÇÃO DE RISCOS

Risco	Descrição	Fase	Aspecto
RE-01	Atraso na execução dos serviços devido à inadequação do ambiente operacional da Funasa	Execução	Qualidade, Custo, Cronograma

RE-02	Ocorrência de ato antieconômico	Execução	Custo
RE-03	Falha na gestão de recursos e sistemas de segurança da informação da Funasa	Execução	Organizacional
RE-04	Pagamentos indevidos ou superfaturados pelos serviços contratados	Execução	Custo
RE-05	Solução contratada não atender às necessidades de negócio	Execução	Escopo, Qualidade, Custo
RE-06	Proposta da contratada deixa de ser a mais vantajosa ao longo da execução do contrato	Execução	Custo
RE-07	Necessidade de ajustes no contrato durante sua execução	Execução	Escopo, Qualidade, Custo
RE-08	Conluio entre fornecedores durante a vigência dos contratos	Execução	Custo
RE-09	Falta de transferência de conhecimento entre a equipe de planejamento da contratação e a de gestão de contratos	Execução	Organizacional
RE-10	Insuficiência de servidores para a gestão de contratos	Execução	Organizacional
RE-11	Descontinuidade do contrato	Execução	Organizacional, Cronograma
RE-12	Baixa efetividade na transferência do conhecimento da contratada para a Funasa	Execução	Organizacional, Qualidade
RE-13	Descumprimento de termos contratuais por parte da contratante	Execução	Qualidade, Cronograma
RE-14	Descumprimento de termos contratuais por parte da contratada	Execução	Qualidade, Cronograma
RE-15	Alta rotatividade de funcionários da contratada responsável pela execução dos serviços	Execução	Qualidade, Cronograma
RE-16	Alto nível de absenteísmo de funcionários da contratada responsável pela execução dos serviços	Execução	Qualidade, Cronograma
RE-17	Adequação de contratos em decorrência de mudanças na legislação que possam afetar a forma de execução ou controle das soluções contratadas	Execução	Qualidade, Custo, Cronograma
RE-18	Conhecimento técnico dos servidores insuficiente para controlar e extrair os benefícios das soluções contratadas	Execução	Organizacional, Qualidade, Custo

4. ANÁLISE DE RISCOS

4.1. A análise de riscos, apresentada na tabela 2, engloba a avaliação da probabilidade de ocorrência de cada risco identificado na seção 3, o grau de impacto caso o risco se concretize e uma descrição sucinta e não extensiva de danos e consequências associados à concretização do risco.

4.2. Como resultado da aplicação do método de priorização de riscos exposto na seção 2, também consta na tabela 2 o nível de prioridade para tratamento dos riscos identificados, bem como a identificação correspondente à categorização por cores.

TABELA 2. ANÁLISE DE RISCOS

Risco	Probabilidade	Impacto	Dano/Consequência
RE-01	Baixo	Alto	• Atraso na execução dos serviços e na entrega de relatórios; • Possível aumento de custo dos projetos que dependem da adequação de ambiente; • Possível queda na qualidade dos serviços durante a adequação de ambiente.
RE-02	Médio	Médio	• Aumento de custos para a administração pública; • Dispêndio de recursos desproporcional ao retorno proporcionado pelas soluções.
RE-03	Baixo	Alto	• Ocorrência de eventos nocivos à Funasa, como brechas de segurança e vazamento de informações.

RE-04	Baixo	Alto	• Aplicação indevida de recursos públicos; • Eventuais sanções a servidores envolvidos na gestão das contratações.
RE-05	Baixo	Alto	• Dispêndio de recursos sem o adequado retorno; • Atraso no atendimento das demandas das áreas de negócio da Funasa.
RE-06	Médio	Alto	• Aumento de custos para a administração pública.
RE-07	Baixo	Alto	• Atraso no alcance dos resultados pretendidos com as contratações; • Perda de capacidade de atendimento às demandas de TI da Funasa.
RE-08	Baixo	Alto	• Aumento de custos para a administração pública; • Ocorrência de eventos como brechas de segurança e vazamento de informações.
RE-09	Baixo	Médio	• Execução incompleta do que foi estabelecido no planejamento da contratação; • Capacidade parcial de execução do serviço pela equipe local.
RE-10	Alto	Médio	• Fiscalização deficitária por excesso de atividades.
RE-11	Baixo	Alto	• Interrupção dos serviços de TI na Funasa.
RE-12	Baixo	Médio	• Perda de conhecimento relevante para a Funasa; • Eventual interrupção dos serviços.
RE-13	Baixo	Alto	• Execução inadequada do objeto dos contratos; • Comprometimento da qualidade dos serviços entregues às áreas gestoras; • Atraso na execução dos serviços e na entrega de relatórios; • Eventual interrupção dos serviços; • Insatisfação das áreas de negócio da Funasa com a CGMTI.
RE-14	Baixo	Alto	• Execução inadequada do objeto dos contratos; • Comprometimento da qualidade dos serviços entregues às áreas gestoras; • Atraso na execução dos serviços e na entrega de relatórios; • Eventual interrupção dos serviços; • Insatisfação das áreas de negócio da Funasa com a CGMTI.
RE-15	Médio	Alto	• Atraso na execução dos serviços e na entrega de relatórios; • Eventual interrupção dos serviços; • Insatisfação das áreas de negócio da Funasa com a CGMTI.
RE-16	Baixo	Alto	• Atraso na execução dos serviços e na entrega de relatórios; • Eventual interrupção dos serviços; • Insatisfação das áreas de negócio da Funasa com a CGMTI.
RE-17	Baixo	Alto	• Aumento de custos para a administração pública; • Atraso na execução dos serviços e na entrega de relatórios; • Comprometimento da qualidade dos serviços entregues às áreas gestoras.
RE-18	Médio	Alto	• Dispêndio de recursos sem o adequado retorno; • Execução inadequada do objeto dos contratos; • Comprometimento da qualidade dos serviços entregues às áreas gestoras; • Perda de conhecimento relevante para a Funasa.

5. TRATAMENTO DE RISCOS

5.1. Na tabela 3 segue o tratamento dos riscos identificados e analisados nas seções anteriores, contemplando a descrição sucinta de ações a serem adotadas com o objetivo de tratar os riscos conforme as estratégias apresentadas na seção 2.

5.2. Para cada risco está registrado o tipo de ação de tratamento, ações para prevenção de danos e consequências, caso o risco se concretize, bem como ações de contingência a serem adotadas e responsáveis por essas ações.

5.3. As ações identificadas podem ser verdadeiramente pontuais e claramente definidas ou podem até representar um conjunto maior de ações coordenadas, como no âmbito de um projeto. Por essa razão, em alguns casos há mais de um responsável pelas ações identificadas, os quais são atores que participarão na execução dessas atividades.

TABELA 3. TRATAMENTO DE RISCOS

Risco	Resposta	Ação para prevenção	Ação de Contingência	Responsável

RE-01	Mitigar	• Identificar necessidades de adequação do ambiente da Funasa antes dessa ação entrar no caminho crítico dos projetos que dela dependem; • Elaborar cronogramas de atividades ou projetos específicos para a adequação de ambiente da Funasa de forma a minimizar o impacto sobre o prazo de entregas das soluções. • Utilização de estimativa de 3 pontos para estimativa do valor inicial do pregão, que diminui o risco de lances iniciais divergentes aos valores praticados no mercado (ETP).	• Adotar estratégias emergenciais para adequação do ambiente conforme o impacto que o prazo para conclusão dessa ação tiver sobre os projetos que dela dependem	CGLOG, CGMTI
RE-02	Evitar	• Levantar soluções de mercado e preços junto ao maior número de fontes possível, como fornecedores e outras licitações; • Registrar os procedimentos adotados para se obter as estimativas a partir dos preços coletados, anexando as evidências das pesquisas realizadas; • Avaliar se os preços estimados das contratações são compatíveis com os resultados pretendidos.	• Anular o processo licitatório caso seja verificado que as estimativas de preços obtidas não são compatíveis com valores médios de contratações similares	CGMTI, CGLOG
RE-03	Mitigar	• Disponibilizar para os fornecedores o que for pertinente no que se refere à Política de Classificação da Informação (PCI), à Política de Controle de Acesso (PCA), ao Plano de Segurança da Informação (PSI) e a Lei Geral de Proteção de Dados (LGPD); • Estabelecer exigências contratuais que obriguem os fornecedores a obedecerem a PCI, a PCA, o PSI e a LGPD; • Executar auditorias de segurança internas referentes ao objeto contratado.	• Aplicar as sanções cabíveis, caso sejam detectadas irregularidades	CGMTI, CGLOG
RE-04	Evitar	• Definir durante o planejamento da contratação itens de verificação para os aceites provisórios e definitivos; • Estabelecer no processo de gestão contratual a checagem de itens de verificação como uma das etapas das quais dependem o recebimento e o respectivo pagamento	• Não pagar por serviços executados sem os devidos aceites	CGMTI, CGLOG
RE-05	Evitar	• Estimular a participação das áreas de negócio quando da identificação das demandas para especificação das contratações; • Apresentar às áreas de negócio o seu papel e a sua importância nas solicitações de demandas dos serviços contratados; • Realinhar as expectativas das áreas de negócio acerca das soluções contratadas;	• Aplicar as sanções cabíveis, caso sejam detectadas irregularidades; • Publicar normativo definindo quem é o gestor de cada solução de TI e suas obrigações; • Celebrar aditivos contratuais objetivando	CGMTI, CGLOG

		• Elaborar os artefatos de planejamento da contratação conforme estabelecido no projeto referente às contratações	atender demandas não previstas; • Realizar novo processo licitatório para contratar soluções capazes de atender às demandas	
RE-06	Mitigar	• Registrar os procedimentos adotados para se obter as estimativas a partir dos preços coletados, anexando as evidências das pesquisas realizadas; • Atualizar pesquisa de levantamento de preços antes de celebrar aditivos contratuais que contemplem aumento de preços unitários em relação às contratações iniciais.	• Realizar novo processo licitatório caso seja constatado prejuízo à Funasa em razão de desequilíbrio econômico financeiro no contrato	CGLOG, CGMTI
RE-07	Mitigar	• Elaborar os artefatos de planejamento da contratação conforme estabelecido no projeto referente às contratações; • Celebrar aditivos contratuais objetivando atender demandas não previstas. • Adequar o catálogo de serviços.	• Realizar novo processo licitatório para contratar soluções capazes de atender às demandas, caso os fornecedores contratados não aceitem os novos termos.	CGMTI, CGLOG
RE-08	Mitigar	• Manter processos de trabalho que contemplem atividades capazes de minimizar a chance de fornecedores atuarem em conluio e causarem danos à Funasa; • Realizar diligências durante a gestão de contratos com vistas a apurar suspeitas de conluio entre fornecedores.	• Aplicar as sanções cabíveis, caso sejam detectadas irregularidades; • Cancelar contratos com base nas irregularidades constatadas; • Iniciar novo processo de contratação para substituição de fornecedores	CGMTI, CGLOG
RE-09	Evitar	• Reunir as equipes de planejamento da contratação - EPC e de gestão de contrato antes da assinatura dos contratos; • Incluir a equipe de gestão de contratos nas reuniões de alinhamento de entendimentos e expectativas com os fornecedores.	• Disponibilizar para a equipe de gestão de contratos todos os artefatos produzidos durante o planejamento das contratações	EPC, CGLOG
RE-10	Mitigar	• Alocar mais servidores para a gestão de contratos; • Qualificar servidores para a gestão de contratos.	• Alocar servidores que sejam responsáveis por gestão de outros contratos.	CGLOG
RE-11	Mitigar	• Elaborar os artefatos de planejamento da contratação conforme estabelecido no projeto referente à contratação.	• Reiniciar o processo de contratação; • Realizar contratação emergencial de fornecedores.	CGMTI, CGLOG
RE-12	Mitigar	• Aceitar entregas somente após a conclusão das ações referentes à transferência de conhecimento	• Recusar entregas em desconformidade com as estratégias de transferência de conhecimento estabelecidas nos contratos;	CGLOG, CGMTI

			• Aplicar as sanções cabíveis, caso sejam detectadas irregularidades; • Cancelar contratos com base nas irregularidades constatadas; • Iniciar novo processo de contratação para substituição de fornecedores	
RE-13	Mitigar	• Planejar e executar ações indispensáveis para a adequada execução dos contratos por parte dos fornecedores	• Cancelar contratos com base nas irregularidades constatadas; • Buscar soluções para minimizar o impacto da ausência das soluções canceladas para a Funasa;	CGLOG, CGMTI
RE-14	Mitigar	• Aplicar as sanções cabíveis previstas em contratos	• Cancelar contratos com base nas irregularidades constatadas; • Iniciar novo processo de contratação para substituição de fornecedores	CGLOG, CGMTI
RE-15	Transferir	• Aplicar as sanções cabíveis previstas em contratos; • Garantir o cumprimento das ações referentes à transferência de conhecimento	• Priorizar alocação de servidores da Funasa para atendimento dos sistemas críticos	CGLOG, CGMTI
RE-16	Aceitar	• Adequar os termos contratuais com consenso das contratadas	• Cancelar contratos com fornecedores que não aceitarem os novos termos contratuais; • Iniciar novo processo de contratação para substituição de fornecedores	CGLOG, CGMTI
RE-17	Mitigar	• Repasse de conhecimento das soluções contratadas; • Qualificar em gestão de contratos servidores tecnicamente capacitados nas áreas de conhecimento das soluções contratadas	• Alocar para a gestão das soluções contratadas servidores que sejam responsáveis pela gestão de outros contratos de objetos similares	CGLOG, CGMTI
RE-18	Mitigar	• repasse de conhecimento das soluções contratadas	• Alocar servidores que sejam tecnicamente capazes de absorver o conhecimento técnico contratado • Capacitação continuada dos envolvidos na execução e fiscalização	CGLOG, CGMTI

Por se tratar de um contrato com serviço estruturante e indispensável para a execução das políticas públicas da Funasa, optamos pela renovação do contrato e manutenção dos serviços.

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.

O presente documento segue assinado pelo Fiscal Técnico, Fiscal Requisitante, Gestor do contrato e Fiscal Administrativo, nos termos da Portaria nº 5274, de 14 de Outubro de 2022 (SEI nº 4176480), em conformidade à *IN 01/2019 SLTI, Art. 38, inc. capt. 3°. incisos I e II.*

GLEICY KELLEN DOS SANTOS FAUSTINO

Integrante Técnico

ANDRÉ WILSON PIMENTA SANTANA

Integrante Requisitante

MARCEL JUNIO MONTEIRO

Integrante Administrativo

Documento assinado eletronicamente por **Andre Wilson Pimenta Santana**, **Integrante Requisitante**, em 26/10/2022, às 15:01, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Gleicy Kellen dos Santos Faustino**, **Integrante Técnico**, em 26/10/2022, às 15:28, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Marcel Junior Monteiro**, **Integrante Administrativo**, em 11/11/2022, às 15:39, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.funasa.gov.br/consulta, informando o código verificador **4197200** e o código CRC **77774A80**.

Referência: Processo nº 25100.006254/2021-77 SEI nº 4197200