

Matriz de Gerenciamento de Riscos

1. Informações Básicas

Número da Matriz de Alocação de Riscos

9/2025

Objeto da Matriz de Riscos

Registro de preços para uma eventual contratação de solução de FIREWALL para a ANM.

Responsável pela Edição

CLAUDIO PEREIRA

Data de Criação

25/03/2025 14:43

2. Histórico de Revisões

Nenhuma Revisão encontrada.

3. Riscos Identificados

Número	Risco	Causa do Risco	Fase	Alocado para	Nível do Risco (I x P)	Nº Item
R-01	Contingenciamento de recursos financeiros para aquisição de solução de NGFW em substituição à atual.	Contingenciamento de recursos financeiros para aquisição de solução de NGFW substituição à atual.	Planejamento	Administração	Alto	

Impactos

1 Dano potencial: Atraso no planejamento e execução de medidas críticas de segurança da rede. Impacto: Médio (impacto técnico, mas não compromete diretamente a cibersegurança). • Impacto: Médio. Afeta o cronograma e planejamento técnico, mas não compromete diretamente a cibersegurança. • Probabilidade: Média. Há riscos administrativos e financeiros que podem influenciar a execução

Ações Preventivas

P-01	Planejamento detalhado de orçamento anual com aprovação prévia e monitoramento financeiro.	Responsáveis: CLAUDIO PEREIRA, MARCIO JOSE ANTUNES GOMES, NEWTON TAKESHI OKUNO
------	--	---

Ações de Contingência

C-01	Realocação de recursos de áreas menos críticas ou reavaliação de prioridades do orçamento.	Responsável: CLAUDIO PEREIRA
------	--	-------------------------------------

C-02	Garantir a extensão temporária do suporte para equipamentos atuais enquanto se aguarda a aquisição da nova solução.	Responsáveis: CLAUDIO PEREIRA, MARCIO JOSE ANTUNES GOMES
------	---	---

Número	Risco	Causa do Risco	Fase	Alocado para	Nível do Risco (I x P)	Nº Item
R-02	Falha em artefatos documentais do processo de contratação de soluções de TIC.	do Falha em artefatos documentais do processo de contratação de soluções de TIC.	do Planejamento	Administração	Baixo	

Impactos

1 Dano potencial: Suspensão ou invalidação do processo licitatório, atrasando o cronograma. Impacto: Médio (impacto técnico com retrabalho, mas sem comprometer a cibersegurança). • Impacto: Médio. Pode atrasar o processo e gerar retrabalho, sem comprometer diretamente a cibersegurança. • Probabilidade: Baixa. Pode ser mitigada com revisões detalhadas

Ações Preventivas

P-01	Revisão minuciosa dos documentos por equipe especializada com checklist de conformidade.	Responsáveis: NEWTON TAKESHI OKUNO, CLAUDIO PEREIRA, MARCIO JOSE ANTUNES GOMES
------	--	---

Ações de Contingência

C-01	Identificação e retificação de falhas documentais com retomada do processo licitatório.	Responsáveis: NEWTON TAKESHI OKUNO, CLAUDIO PEREIRA, MARCIO JOSE ANTUNES GOMES
------	---	---

C-02 Contratação emergencial de serviços temporários para mitigação de falhas até a regularização do processo. **Responsável:** CLAUDIO PEREIRA

Número	Risco	Causa do Risco	Fase	Alocado para	Nível do Risco (I x P)	Nº Item
R-03	Demora no processo de contratação de serviço de NGFW.	no de Demora no processo de contratação de serviço de NGFW.	Planejamento	Administração	Médio	

Impactos

Dano potencial: Prolongamento do uso de soluções obsoletas e aumento do risco de falhas de segurança. Impacto: Alto (compromete

1	diretamente a cibersegurança). • Impacto: Alto. Prolonga a exposição a falhas técnicas e compromete a capacidade de defesa. • Probabilidade: Média. Depende da complexidade e eficiência do processo licitatório.	
Ações Preventivas		
P-01	Cronograma claro com metas intermediárias e monitoramento frequente do processo de aquisição.	Responsáveis: CLAUDIO PEREIRA, MARCIO JOSE ANTUNES GOMES
Ações de Contingência		
C-01	Adoção de medidas provisórias, como ampliação do suporte atual ou soluções temporárias de segurança.	Responsáveis: CLAUDIO PEREIRA, MARCIO JOSE ANTUNES GOMES
C-02	Implementar soluções baseadas em serviços de segurança na nuvem para proteção temporária	Responsáveis: CLAUDIO PEREIRA, MARCIO JOSE ANTUNES GOMES

Número	Risco	Causa do Risco	Fase	Alocado para	Nível do Risco (I x P)	Nº Item
R-04	Uso de firewall sem suporte e atualização.	O risco "Uso de firewall sem suporte e atualização" decorre da utilização de um appliance de segurança sem garantia contratual vigente, representando uma vulnerabilidade técnica atual e persistente.	Planejamento	Administração	Extremo	
		Essa condição não se limita apenas à fase de planejamento da nova contratação, mas impacta diretamente a segurança da infraestrutura de rede, expondo a organização a potenciais falhas de segurança e comprometendo a proteção dos ativos digitais até a efetiva contratação de uma nova solução.				
Impactos						
1	Compromete diretamente a cibersegurança da rede da Agência levando a uma falha sistêmica de toda a Agência.					
Ações Preventivas						
P-01	Contratação de nova solução de firewall.			Responsáveis: FABIO FERNANDO BORGES, CLAUDIO PEREIRA		
Ações de Contingência						
C-01	Contratação emergencial de firewall como serviço (FaaS) ou de suporte estendido.			Responsáveis: FABIO FERNANDO BORGES, CLAUDIO PEREIRA		

Número	Risco	Causa do Risco	Fase	Alocado para	Nível do Risco (I x P)	Nº Item
R-05	Potencial ataque de ransomware por conta de firewall desatualizado.	Esse risco evidencia uma grave vulnerabilidade de segurança cibernética, onde a obsolescência do firewall aumenta significativamente a exposição da infraestrutura digital a ameaças de sequestro de dados. A desatualização do equipamento de proteção perimetral, que é a primeira medida de contenção de segurança da rede, cria brechas que podem ser exploradas por cibercriminosos, potencializando o risco de interrupções operacionais, perdas financeiras e comprometimento de informações sensíveis da Agência. Esse risco também não se limita à fase de planejamento da contratação.	Planejamento	Administração	Extremo	
Impactos						
1	Esse tipo de ataque leva a uma falha sistêmica total, paralisando toda a infraestrutura de TI da Agência por período indeterminado, levando a perda parcial ou total de todos os dados e ativos da rede da ANM.					
Ações Preventivas						
P-01	Utilização de solução de firewall e atualização contínua de políticas de segurança, backup e monitoramento de vulnerabilidades. Responsáveis: Fabio Fernando Borges, CLAUDIO PEREIRA					
Ações de Contingência						
C-01	Contratação de forma emergencial de serviços de segurança (como SOCs 24/7) e ferramentas de contenção de ataques (microsegmentação, XDR e NDR). Responsáveis: Fabio Fernando Borges, CLAUDIO PEREIRA					
C-02	Ativação imediata de plano de resposta a incidentes com recuperação via backups seguros Responsáveis: FABIO FERNANDO BORGES, CLAUDIO PEREIRA					

4. Acompanhamento das Ações de Tratamento de Riscos

Nenhum acompanhamento incluído.

5. Responsáveis / Assinantes

CLAUDIO PEREIRA

Integrante Requisitante

MARCIO JOSE ANTUNES GOMES

Integrante Técnico

NEWTON TAKESHI OKUNO

Integrante Administrativo

FABIO FERNANDO BORGES

Autoridade competente