MAPA DE GERENCIAMENTO DE RISCO (MGR) Nº 2/2025/SETRAN

A seguir, a planilha com os principais riscos, sua descrição, a avaliação do nível de risco e as medidas mitigado cada variável:

Núm.	Aspecto/variável	Descrição do risco	Nível de risco	Comentários/mitigações
1	Segurança de Dados	Risco de acesso não autorizado, vazamento ou interceptação de informações confidenciais do TRE, falhas na criptografia e controles de acesso inadequados.	Alto	- Implantar protocolos robustos de criptografia e autenticação. - Utilizar controles de acesso rigorosos e monitoramento contínuo do ambiente.
2	Treinamento e Capacitação do Pessoal	Risco de que o treinamento seja insuficiente ou mal estruturado, resultando em baixa adesão, erros operacionais e uso inadequado dos sistemas.	Médio	- Elaborar um cronograma de capacitação detalhado. - Realizar avaliações periódicas de desempenho e reciclagem de treinamento conforme necessário.
3	Fornecimento e Manutenção dos Equipamentos	Risco de atrasos na entrega, equipamentos com defeito ou manutenção inadequada que comprometam o funcionamento do sistema, afetando a operação de monitoramento.	Alto	- Estabelecer SLAs[1] rigorosos para entrega e manutenção. - Implementar planos de manutenção preventiva e contingência para equipamentos críticos.

4	Continuidade dos Serviços	Risco de interrupção do serviço – especialmente em áreas sem sinal – devido a falhas na transmissão de dados ou problemas no funcionamento do sistema via satélite.	Alto	- Adotar redundâncias (ex.: comunicação via satélite e outros canais). - Realizar testes de estresse[2] e simulações de falhas para assegurar a continuidade.
5	Cumprimento de Prazos	Risco de atrasos na contratação, implantação e homologação do sistema, não atingindo o prazo de operação plena até maio de 2025.	Médio	- Acompanhamento rigoroso do cronograma do projeto. - Inclusão de cláusulas contratuais de penalidade para atrasos e gestão de riscos no planejamento.
6	Custos e Orçamentos	Risco de exceder o orçamento e custos extras decorrentes de imprevistos, variações de preços ou de exigências tecnológicas não previstas inicialmente.	Médio	- Elaborar orçamento detalhado com margens de contingência. - Monitorar periodicamente os custos e revisar o planejamento financeiro do projeto.
7	Integridade dos Dados	Risco de corrupção, perda ou alteração indevida dos dados durante o armazenamento, transmissão ou backup, comprometendo a confiabilidade das informações.	Alto	- Implementar backups regulares e redundantes. - Realizar auditorias e testes de integridade dos dados periodicamente.
8	Conformidade com Normas e Regulamentações	Risco de não conformidade com os requisitos legais e normativos do setor público, o que pode impactar a licitação e a validade dos processos contratuais.	Médio	- Revisão jurídica contínua do projeto. - Adequação aos padrões e normas vigentes, com monitoramento das atualizações legislativas.
9	Suporte e Monitoramento (Central de Monitoramento)	Risco de falhas na central de monitoramento, atrasos na resposta a incidentes ou insuficiência do suporte técnico, prejudicando a operação do sistema.	Médio	- Estabelecer SLAs específicos para a central de monitoramento. - Treinar os operadores e definir procedimentos claros para resposta a incidentes.

10	Dependência de Terceiros (Operadora Satelital)	Risco de interrupções ou falhas no serviço fornecido por parceiros terceiros (como operadoras de satélite e telecomunicações), que podem afetar a transmissão de dados.	Alto	- Firmar contratos com fornecedores reconhecidos e com histórico de confiabilidade. - Prever acordos de redundância e monitoramento contínuo dos serviços.
11	Vulnerabilidades Técnicas	Risco de bugs, vulnerabilidades de software ou falhas sistêmicas que possam ser exploradas, comprometendo a segurança e a funcionalidade do sistema.	Alto	- Realizar testes de penetração[3], atualizações e auditorias de segurança de forma contínua. - Implementar uma política de correções rápidas (patch management[4]).

1. **SLAs (Service Level Agreements):** SLAs ou Acordos de Nível de Serviço, são contratos ou acordos forr definem os padrões mínimos de qualidade e desempenho que um serviço deve atender. Eles especific exemplo, tempos de resposta, disponibilidade, taxas de resolução de problemas e outros parâmetros crít garantem que o serviço prestado atenda às necessidades do cliente. **No contexto da cen monitoramento**, um SLA pode definir que, em caso de incidentes, a resposta deve ser iniciada em minutos e a solução final em, no máximo, 2 horas.
2. **Teste de Estresse:** um teste de estresse é um procedimento que avalia a capacidade e a robustez sistema ou aplicação submetendo-o a condições extremas de carga ou funcionamento, além dos níveis de operação. O objetivo é identificar o ponto de falha ou os limites operacionais, garantindo que o sistem lidar com situações de sobrecarga sem comprometer a continuidade dos serviços.

3. **Teste de Penetração:** o teste de penetração, ou *pen test*, é uma simulação controlada de ataque sistema, rede ou aplicação com o intuito de identificar e explorar vulnerabilidades de segurança. Ele verificar a eficácia das defesas implementadas e identificar pontos fracos que possam ser explora agentes mal-intencionados.

4. **Patch Management:** é o processo de gerenciar e aplicar atualizações (patches) de software e firmw sistemas e dispositivos. Essas atualizações têm como objetivo corrigir vulnerabilidades, bugs e me segurança e a performance dos sistemas.
   Etapas envolvidas:
   - **a) Identificação:** Monitoramento de novos patches disponibilizados pelos fornecedores.
   - **b) Teste:** Verificação em ambiente controlado para assegurar que o patch não cause conflitos.
   - **c) Implementação:** Aplicação do patch no ambiente de produção.
   - **d) Monitoramento:** Verificação pós-implementação para confirmar a eficácia e estabilidade da c

Considerações Finais

Integração dos Sistemas: A complexidade do serviço (que abrange desde a transmissão de dados via r tecnologias até a integração com a central de monitoramento) exige que os riscos sejam monitorados d integrada.

Planos de Contingência: É fundamental que, para cada risco identificado, existam planos de contingência e de revisão para corrigir desvios ou imprevistos.

Governança: Uma estrutura de governança, envolvendo comitês de monitoramento e comunicação constante TRE e a empresa contratada, será decisiva para o sucesso do projeto.

Manaus/AM, Data da Assinatura Eletrônica

ANTONIO CARLOS DE CASTRO MOREIRA
ANALISTA JUDICIÁRIO

Documento assinado eletronicamente em **28/02/2025**, às **08:26**, conforme artigo 1º, §2, III, b, da Lei nº 11.419/2006 .

A autenticidade do documento pode ser conferida no site https://sei.tre-am.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0000431015** e o código CRC **F04D4D47**.