TRIBUNAL REGIONAL ELEITORAL DO MARANHÃO

ANEXO

MAPA DE RISCOS

PROCESSO 0003880-26.2025.6.27.8000 (GOOGLE WORKSPACE)

NÚMERO	EVENTO DE RISCO	CAUSA	CONSEQUÊNCIA	CATEGORIA	PROBABILIDADE	IMPACTO	NÍVEL DE RISCO	ESTRATÉGIA	TRATAMENTO (AÇÃO PREVENTIVA)	TRATAMENTO (AÇÃO DE CONTINGÊNCIA)	CONTROLE	PROPRIETÁRIO DO RISCO
1	Falha na segurança da informação	Falta de formalização de termo de responsabilidade e segilo de informações	Vazamento de dados internos da administração	Operacional/Legal	Baixa	Médio	MODERADO	MITIGAR	Formalizar termo de responsabilidade para que o CONTRATANTE assine.	1 - Notificar a empresa para corrigir o problema. 2 - Solicitar aplicação de penalidade, em caso de descumprimento.	Durante a execução do serviço.	SERED
2	Vazamento de informações sensíveis	Configuração inadequada de permissões ou falha humana	Comprometimento da confidencialidade institucional	Segurança da Informação	Média	Alto	ALTO	MITIGAR	Implementar políticas rígidas de acesso e revisão periódica de permissões	Afastar conta comprometida, notificar incidentes e auditar acessos Comunicação imediata à Autoridade Nacional de Proteção de Dados Comunicação aos Titulares dos Dados Conteúdo Mínimo da Comunicação (tanto para a ANPD quanto para o titular, com as devidas adaptações) Avaliação do Risco ou Dano Relevante Registro do Incidente Adoção de Medidas Corretivas e de Melhoria Cooperação com a ANPD	Monitoramento com Google Vault e alertas do Admin Console	SERED
3	Indisponibilidade do serviço Google Workspace	Falhas nos datacenters da Google ou ataques DDoS	Interrupção nos serviços de e-mail, agenda, drive e videoconferência	Operacional	Baixa	Muito Alto	MODERADO	MITIGAR	Monitorar status da Google Cloud, criar planos de continuidade de negócio	Utilizar canais alternativos temporários de comunicação	Plano de Continuidade de TIC e canais alternativos (e.g. e-mail institucional em domínio de backup)	SERED
4	Perda de dados armazenados no Drive	Exclusão acidental por usuários ou má configuração da política de retenção	Perda de documentos críticos	Segurança da Informação	Média	Médio	MODERADO	MITIGAR	Implementar política de backup e uso do Google Vault para retenção	Recuperar arquivos via Admin Console ou backup externo	Backup automatizado e controle de exclusões críticas	SERED
5	Uso indevido por colaboradores	Acesso a serviços para fins pessoais ou fora da política institucional	Riscos de imagem, segurança e uso indevido de recursos	Conformidade	Média	Médio	MODERADO	MITIGAR	Implementar políticas de uso aceitável e auditoria de comportamento	Aplicar sanções administrativas e reconfigurar contas	Política de Uso Aceitável e trilhas de auditoria	SERED
6	Falta de capacitação dos usuários	Mudança na plataforma ou recursos pouco explorados	Subutilização das funcionalidades e insatisfação com o serviço	Capacitação	Alta	Médio	ALTO	MITIGAR	Oferecer treinamentos periódicos e guias de boas práticas	Suporte técnico ampliado e apoio remoto pontual	Programa interno de capacitação e canal de dúvidas	NSI
7	Acesso indevido por contas comprometidas	Phishing, uso de senhas fracas ou reutilizadas	Roubo de dados, envio de e-mails falsos	Segurança da Informação	Média	Alto	ALTO	MITIGAR	Implementar autenticação de dois fatores (2FA) e política de senhas	Suspender conta, redefinir credenciais e notificar incidente	Força de senha, 2FA e alertas de login suspeito	SESEC
8	Limitações de armazenamento	Consumo elevado por parte dos usuários sem política de gestão	Interrupção no envio/recebimento de e-mails ou armazenamento de arquivos	Operacional	Baixa	Médio	MODERADO	MITIGAR	Definir cotas de armazenamento e política de limpeza	Adquirir espaço adicional ou excluir dados obsoletos	Monitoramento de uso via Admin Console	SERED
9	Exposição acidental de documentos	Compartilhamento incorreto ou falta de restrição de acesso	Acesso não autorizado a documentos internos	Segurança da Informação	Alta	Alto	ALTO	MITIGAR	Treinar usuários sobre práticas de compartilhamento seguro	Revogar compartilhamentos e restringir domínios externos	Alertas de compartilhamento e política de domínio	SERED
10	Dependência excessiva da conectividade com a internet	Quedas frequentes de conexão ou baixa qualidade de rede	Interrupção total de acesso à plataforma	Infraestrutura	Média	Alto	ALTO	MITIGAR	Garantir redundância de links e estabilidade da rede local	Redirecionar usuários para conexões alternativas ou locais	Monitoramento de rede e plano de contingência local	SERED
11	Dependência tecnológica do fabricante	Possibilidade do TRE-MA se tornar excessivamente dependente da Google para uma tecnologia, produto ou serviço	Dificuldades para mudar de fornecedor, custos elevados, falta de flexibilidade. Vulnerabilidade a mudanças na política de preços Descontinuação de produtos/suporte ou queda na qualidade do serviço do fornecedor	Operacional/Legal	Baixa	Alto	BAIXO	MITIGAR	1. Através de uma análise comparativa, optar por padrões abertos e Interoperabilidade, possibilitaria maior independência tecnológica a longo prazo, porém com elevado custo de transição, suporte limitado e riscos aumentados de indisponibilidade e falhas de segurança 2. Análise Contratual: Incluir cláusulas que garantam a portabilidade dos dados, acesso a APIs, e condições razoáveis para término ou transição de contrato. 3. Desenvolvimento de Conhecimento Interno: Investir na capacitação da equipe interna para reduzir a dependência do suporte técnico e conhecimento exclusivo do fornecedor 4. Monitoramento Contínuo do Mercado: Manter-se atualizado sobre alternativas tecnológicas e novos fornecedores que possam surgir 5. Exigir Transparência na Política de Evolução: Solicitar clareza sobre o roadmap da solução, políticas de atualização, custos futuros e compatibilidade com versões anteriores.	Para Ação 1: 1.1. No ETP (requisitos técnicos) demonstra-se que que haveria elevado custo de implantação, customização, operação e manutenção. Para Ação 2: 2.1. Envolver a assessoria jurídica na elaboração/análise das minutas contratuais para inclusão de cláusulas de saída, portabilidade de dados (formatos, prazos, custos) e propriedade intelectual. 2.2. No ETP está especificado a necessidade de documentação técnica completa da solução. Para Ação 3: 3.1. Caso seja necessário, o conhecimento técnico pode ser repassado através de material de apoio como tutorial. Para Ação 4: 4.1. Estabelecer um processo de revisão periódica (ex: anual) das soluções contratadas e das alternativas de mercado. Para Ação 5: 5.1. No ETP, dentre os Principais Componentes e Funcionalidades, a solução contratada deverá abranger Suporte técnico e atualizações contínuas nativas do modelo SaaS, sem custos adicionais 5.2. Incluir em contrato a Manutenção e atualização de softwares e hardwares que compõem a solução ofertada.	Monitoramento Contínuo dos Indicadores de Risco (KRIs) Revisões Periódicas da Matriz de Riscos e das Ações de Mitigação Análise de Impacto de Mudanças e Novas Versões Planejamento e Simulação de Estratégias de Saída (Exit Strategy) Auditorias Periódicas Canais de Feedback e Reporte	SERED
12	Desatualização de configurações administrativas	Mudanças na política da Google não aplicadas localmente	Vulnerabilidades ou não conformidade com padrões atuais	Governança	Média	Alto	ALTO	MITIGAR	Acompanhar atualizações da plataforma e revisar configurações trimestralmente	Atualizar manualmente ou solicitar suporte Google	Checklist de governança e revisão periódica	SERED

PLANO DE TRATAMENTO DE RISCOS DO MACROPROCESSO DE CONTRATAÇÃO 0002960-23.2023.6.27.8000 (2374669)

Os macrorriscos seguem a Política de Gestão de Riscos do TRE-MA que visa padronizar níveis de riscos do Macroprocesso de Contratação.

0006295-79.2025.6.27.8000 2510346v3