GOVERNO DO ESTADO DE RONDÔNIA
Secretaria de Estado da Educação - SEDUC

MAPA DE RISCO

CONSIDERANDO , o Decreto nº. 23.277, de 16 de outubro de 2018 em seu artigo 2º inciso V que trata do Órgão Central de Controle na qualidade de segunda linha de defesa constituída pelas funções de supervisão, monitoramento e **assessoramento quanto a aspectos relacionados aos riscos** e controles internos da gestão do órgão ou entidade.

CONSIDERANDO, a Portaria nº 217 de 08 de dezembro de 2021, que estabelece a metodologia de gestão de risco no âmbito do Poder Executivo Estadual;

CONSIDERANDO, a Portaria 1662 (0057089972), que designa Comissão Especial destinada a realizar estudo técnico preliminar relativo a contratação de serviço de fornecimento de solução de equipamentos Firewall de Aplicação Web - WAF, proteção das aplicações disponibilizadas na modalidade web, dos ativos de hardware e software e das aplicações Web da SEDUC-RO, compreendendo fornecimento de equipamentos (appliances) e suas respectivas licenças de suporte e atualização, conforme descrito no Documento de Formalização de Demanda - DFD 202 (0056682019).

CONSIDERANDO, a orientação sobre análises e matriciamento de riscos à luz da Lei nº 14.133/2021 e Decreto 28/874/2024, estabelecida Coordenadoria de Controle Interno, por meio da Gerência de Gestão de Risco, nos autos do processo SEI (0029.019419/2024-01).

1. DA CONTEXTUALIZAÇÃO

O objetivo é consolidar um relatório abrangente que será apresentado à Alta Gestão, trazendo consigo soluções concretas e estratégicas.

Ainda, é relevante mencionar que o Decreto N. 23.277, de 16 de outubro de 2018, delineia claramente as linha de defesa, bem como o conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações.

Esta estrutura contribui significativamente para a eficácia dos processos e a garantia da conformidade com as diretrizes estabelecidas.

2. DA METODOLOGIA UTILIZADA

Para atender a presente demanda, bem como subsidiar a Secretaria de Estado da Educação - SEDUC em sua tomada de decisão, será utilizada a metodologia de consultoria da CGE/RO, disposta na Portaria nº 217 de 08 de dezembro de 2021, que está em consonância com o disposto na Instrução Normativa n° 05, de 25 de maio de 2017.

Para elaboração desta nota é importante noticiar o significado de alguns conceitos que serão adotados:

Risco é o desvio em relação aos objetivos esperados, podendo ser de natureza positiva, negativa ou englobar ambos, abordando oportunidades e ameaças. A Consequência é o desfecho de um evento de risco sobre os objetivos do processo. A Avaliação de Risco, por sua vez, constitui o processo de identificação e análise dos riscos pertinentes que influenciam a realização dos objetivos da organização, delineando a resposta apropriada a cada risco. Este procedimento compreende diversas etapas:

Identificação de Riscos: engloba a busca, identificação e descrição de riscos, incluindo a identificação de suas fontes, causas e possíveis consequências. Este processo pode envolver dados históricos, análises teóricas, insights de especialistas e partes interessadas;

Análise de Riscos: implica na compreensão das causas e consequências imediatas, incorporando uma consideração detalhada das incertezas, fontes de risco, cenários, bem como dos controles e sua eficácia;

Classificação de Níveis de Risco: estabelece o nível de risco operacional através do produto da avaliação de impacto pela avaliação de probabilidade, conforme definido pelos parâmetros estabelecidos;

Tratamento de Riscos: abrange qualquer medida adotada para gerenciar o risco, que pode incluir a decisão de evitar o risco iniciando ou descontinuando atividades relacionadas a ele; mitigar o risco ao reduzir sua probabilidade de ocorrência e/ou suas consequências (impacto); compartilhar o risco com terceiros; ou aceitar o risco através de uma escolha consciente e justificada."

Assim, serão então analisado os riscos inerentes ao objeto da contratação em comento.

3. DOS OBJETIVOS DA CONTRATAÇÃO

O ambiente educacional depende fortemente de soluções tecnológicas para assegurar a continuidade e a eficiência das atividades acadêmicas e administrativas. Atualmente, todas as unidades escolares e administrativas conectadas ao Data Center da SEDUC, localizado na sede administrativa (CPA), utilizam a rede IP/MPLS e a rede INFOVIA do Governo do Estado de Rondônia. Essas redes são fundamentais para o acesso aos sistemas informatizados da Secretaria e para a comunicação via internet, garantindo a operacionalidade e a qualidade dos serviços educacionais prestados à população.

No entanto, os equipamentos atualmente em operação, adquiridos por meio do Processo SEI nº 0029.135533/2020-45, CONTRATO N° 299/PGE-2020 (0012423252), encontram-se com contratos de garantia e suporte expirados, impossibilitando a renovação mediante simples aditamento, conforme as especificações contratuais do fabricante. Além disso, esses equipamentos não mais atendem às demandas tecnológicas atuais, colocando em risco a segurança e a eficiência da infraestrutura de TI da SEDUC.

Nos últimos anos, ataques cibernéticos direcionados a órgãos públicos e entidades governamentais tornaram-se cada vez mais frequentes e sofisticados. Em 2023, o Brasil registrou diversos incidentes relevantes que evidenciam a vulnerabilidade de instituições públicas. Casos como o ataque ao Supremo Tribunal Federal (STF) e ao Ministério da Saúde em anos anteriores, bem como incidentes recentes envolvendo sistemas de universidades e instituições estaduais, demonstram o impacto significativo que falhas de segurança podem causar.

Esses ataques, frequentemente baseados em ransomware, phishing direcionado e exploração de vulnerabilidades em aplicações web, resultam em paralisações de serviços, vazamento de dados sensíveis e prejuízos financeiros significativos. Relatórios recentes de empresas de segurança indicam que a área da educação está entre os setores mais visados por cibercriminosos devido à grande quantidade de dados armazenados e

ao acesso remoto amplamente utilizado por servidores e alunos.

Diante desse cenário, a adoção de um Firewall de Aplicação Web (WAF) é imprescindível para a SEDUC-RO, pelos seguintes motivos:

- Proteção Contra Ameaças Cibernéticas – Um WAF permite identificar e mitigar ataques avançados, protegendo aplicações web contra ameaças como injeção de SQL, cross-site scripting (XSS) e exploração de vulnerabilidades.
- Garantia da Continuidade dos Serviços Educacionais – A segurança das aplicações web é fundamental para assegurar o acesso ininterrupto aos sistemas educacionais e administrativos, impactando diretamente na qualidade dos serviços oferecidos à população.
- Conformidade com Normas de Segurança – A contratação de soluções modernas está alinhada à Política de Segurança da Informação (PSI), instituída pela Portaria nº 97, de 09 de junho de 2021, da SETIC/RO, que estabelece os princípios de integridade, confidencialidade, autenticidade e disponibilidade.
- Prevenção de Danos Financeiros e Reputacionais – Incidentes de segurança podem comprometer a prestação de serviços essenciais, além de gerar prejuízos financeiros e impactar negativamente a imagem da instituição.
- Elevação da Postura de Segurança – A implementação de uma solução WAF robusta fortalecerá a segurança da informação da SEDUC-RO, protegendo seus ativos críticos e garantindo a continuidade das operações.

Portanto, torna-se imperativo que a SEDUC-RO realize a contratação de uma empresa especializada para o fornecimento de uma solução de Firewall de Aplicação Web (WAF). Essa contratação é essencial para garantir a proteção das aplicações web, salvaguardar informações sensíveis e assegurar a continuidade dos serviços educacionais prestados pelo Governo do Estado de Rondônia.

4. DA AVALIAÇÃO DE RISCO - MAPA DE RISCO

Após a análise documental, tornou-se evidente (conforme ilustrado no quadro abaixo) a identificação de riscos que demandam a atenção e avaliação da alta Administração da SEDUC. Estas ocorrências requerem a devida consideração para a implementação de medidas que visem evitar, mitigar, transferir ou compartilhar tais adversidades.

Neste contexto, à luz das disposições contidas nos artigos 15, 16 e 22 da Portaria nº 217 de 8 de dezembro de 2021, bem como nas tabelas anexas (que abrangem a escala de probabilidades, consequências e níveis de riscos), procederemos com a análise pormenorizada.

Nesse ínterim, e seguindo essa linha de raciocínio, a análise do processo de contratação/aquisição foi conduzida levando em consideração os riscos e possíveis irregularidades mais significativos.

Foram identificados os riscos com maior probabilidade e impacto, e propostas medidas que a Alta Administração pode implementar para gerenciar essas situações.

Ademais, foram destacados outros riscos que também requerem atenção, juntamente com as medidas correspondentes para o seu tratamento.

Insta esclarecer que os riscos, probabilidade / consequências, nível de riscos e ações sugeridas, foram validados de forma consensual entre a equipe da Comissão de Estudo Técnico Preliminar, que constituiu o ponto focal na Secretaria para tratar os assuntos que são objeto desta nota de risco.

5. QUANTO À AVALIAÇÃO GERAL DOS PRINCIPAIS RISCOS E/OU IMPROPRIEDADES IDENTIFICADAS

Ressalta-se que a classificação segundo o nível de risco identificado reflete a percepção da Comissão de Estudo Técnico Preliminar a partir da pesquisas, históricos, dados da instituição levantados e não sinalizado como estanque ou definitivo, cabendo ao gestor a avaliação dos pontos para decidir quanto à aplicação das ações sugeridas ou a adoção de outras que julgar cabíveis.

A ideia é dar suporte a Gestão para que, assim querendo, possam adotar as contribuições abaixo noticiadas.

Em um primeiro momento, é importante salientar que as ações propostas não se restringem exclusivamente a medidas tomadas no momento da contratação.

Isso se baseia na consideração de que a administração tem a liberdade de implementar ações complementares durante a fase de planejamento, execução do serviço ou monitoramento, caso isso resulte em respostas mais efetivas aos riscos identificados.

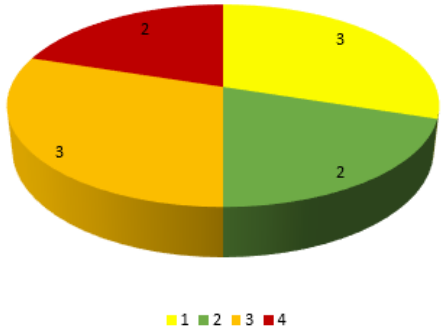
Do quantitativo de 10 (dez) riscos identificados, têm-se, de acordo com o nível de risco estabelecido, 3 (três) considerados baixo, 2 (dois) considerados médio, 3 (três) considerados alto e 2 (dois) considerado extremo, conforme tabela 1 e gráfico 1 abaixo que seguem:

A partir das medidas propostas, almeja-se enriquecer as iniciativas do Governo do Estado.

Isso implica em colaborar ativamente para a redução dos riscos, aprimorar os mecanismos de governança e implementar as melhores práticas em operações, gestão de riscos e controles internos dentro da esfera da SEDUC, especialmente no que tange aos processos de contratação. Isso, por sua vez, visa oferecer suporte à Alta Gestão no processo decisório.

NÍVEL DE RISCO	NÚMERO DE RISCOS	PERCENTUAL
Baixo	3	30%
Médio	2	20%
Alto	3	30%
Extremo	2	20%
TOTAL	10	100%

DISTRIBUIÇÃO DE RISCOS



RISCOS	CAUSAS	PROBABILIDADES	CONSEQUÊNCIAS	NÍVEL DE RISCO	AÇÕES SUGERIDAS	AÇÕES DE CONTINGÊNCIA	ALOCAÇÃO
Falta de clareza e de detalhamento do objeto	Definição imprecisa do objeto em virtude da complexidade técnica dos serviços	Rara	Relevante	Médio	Concentração da força de trabalho na elaboração minuciosa do objeto, com detalhamento, precisão e clareza	Se houver conformidade legal, providenciar aditivo entre as partes.	Contratante
Contratação de empresa sem qualificação econômica-financeira e/ou técnica-operacional para execução do objeto	Definição inadequada dos critérios	Rara	Muito relevante	Alto	Exigência documental apta a comprovar a capacidade técnica e econômica da empresa em arcar com o contrato	Rescisão Contratual	Contratante
Não contratação	Ausência de recursos orçamentários	Raríssima	Relevante	Baixo	Intermediação e gestão com as aréas responsáveis com vistas ao provimento dos recusos necessários	Prover meios emergenciais para contratação	Contratante
Entrega com qualidade inferior à exigida	Contratação de empresa sem a capacidade de executar o contrato	Rara	Relevante	Médio	Descrever no TR a substituição imediata do produto	Aplicar punição	Contratada
Atraso na execução do objeto em razão do descumprimento de prazo por parte da Contratada	Comprometimento do cronograma de execução do objeto e, consequentemente, a relevância do serviço	Rara	Muito relevante	Alto	Elaborar cronograma efetivo e dentro dos parametros relevantes	Monitorar prazos e estabelecer requisitos temporais compativeis com a complexidade do serviço	Contratada
Não manter a proposta ou desistir do contrato	Indisponibilidade do serviço	Rara	Muito relevante	Alto	Pesquisa de preços que represente os preços praticados no mercado	Aplicar punição e realizar nova contratação	Contratada
Contratação com preço acima da média praticada no mercado	Dano ao erário	Raríssima	Relevante	Baixo	Avaliação da composição dos preços unitários propostos.	Utilizar os preços dos Bancos de dados do Governo, avaliar todas as cotações, fazer comparativos para que os preços unitários reflitam a realidade.	Contratante
Não cumprimento das obrigações assumidas pela empresa contratada	Gestão e fiscalização inadequada do contrato	Raríssima	Relevante	Baixo	Acompanhamento da execução do contrato e cumprimento dos prazos estabelecidos	Notificar a empresa, para aplicação de sanções	Contratada

Paralisação dos serviços de redundância - Ambiente de recuperação de desastres de Disaster Recovery (DR)	**Não contratação**	**Eventual**	**Muito relevante**	**Extremo**	**Celeridade na contratação em razão do tempo para expiração do suporte - Março/2025.**	**Procurar suporte junto a Superintendência Estadual de Tecnologia da Informação e Comunicação para alocar recursos das aplicações**	**Contratante**
Perda da garantia que impacta diretamente na manutenção dos serviços de TIC da SEDUC	**Atraso na contratação**	**Eventual**	**Muito relevante**	**Extremo**	**Efetuar uma gestão proativa de garantias que dispõe de alertas automáticos sobre a expiração. Isso garantirá que ações preventivas sejam tomadas antes que a garantia expire.**	**Verificar se há contratos de manutenção ativa ou suporte técnico terceirizado que possam ser ampliados para cobrir os serviços.**	**Contratante**

6. DA CONCLUSÃO

O presente documento encontra-se em total consonância com a Portaria nº 217/2021, CGE/RO, que estabelece a metodologia de gestão de risco no âmbito do Poder Executivo Estadual, o que nos permite destacar que destacar que a Matriz de Riscos apresentada não visa apontar irregularidades nos processos, mas sim identificar possíveis eventos que possam afetar o alcance dos objetivos do processo.

Ademais, propõe ações para mitigar esses riscos, cabendo à gestão avaliar a viabilidade e pertinência de sua implementação.

O foco deste trabalho foi direcionado para a identificação dos principais riscos relacionados a contratação de serviço de fornecimento de solução de equipamentos Firewall de Aplicação Web - WAF, proteção das aplicações disponibilizadas na modalidade web, dos ativos de hardware e software e das aplicações Web da SEDUC-RO, compreendendo fornecimento de equipamentos (appliances) e suas respectivas licenças de suporte e atualização, foram minuciosamente identificados e analisados os riscos, com especial atenção ao saneamento daqueles riscos classificados como de alto e extremo grau, sendo recomendado a apresentação de justificativas e esclarecimentos relevantes caso não sejam adotadas medidas mitigadoras, para evitar possíveis questionamentos de órgãos de controle externo.

Para os riscos classificados como de baixo ou médio impacto, ressalta-se a importância de adotar as melhores práticas disponíveis, mesmo não existindo urgência em no tratamento.

Importa destacar, como anteriormente mencionado, que as informações aqui apresentadas têm o intuito de orientar a atuação do gestor público.

No entanto, cabe à autoridade responsável tomar a decisão que julgar mais apropriada para atender ao interesse público.

Ademais, as orientações e sugestões fornecidas não abrangem todas as possibilidades de identificação de riscos e questões relevantes no processo operacional em questão. É atribuição da unidade e dos gestores das áreas envolvidas adotar uma abordagem contínua para identificá-los, bem como avaliar eventuais fragilidades no processo. Além disso, devem implementar as medidas necessárias, como controles internos eficazes, tanto para corrigir possíveis irregularidades e/ou inadequações, quanto para atuar preventivamente no desenvolvimento de políticas e procedimentos internos, assegurando a conformidade com a legislação, as metas e os objetivos estabelecidos.

Porto Velho, data e assinatura no sistema.

Elaborado por

ANA CAROLINE DIAS COCIUFFO VILLELA
Assessora IX - CAD/SEDUC
******698

AYLLA ROKXANA TRAJANO PEREIRA SOUZA
Matrícula n. ******959

GILSON NEDISON FERREIRA DE SOUZA
Matrícula n. ******261

NELINHO TEIXEIRA NERES
Matrícula n. ******961

LUCIANO DE OLIVEIRA SILVA
Matrícula n. ******983

ANEXO ÚNICO

Escala de probabilidades, consequências e níveis de riscos

Escala de Probabilidade:

Frequência	Significado	Expressão

Raríssima	Evento extraordinário para os padrões conhecidos da gestão e operação do processo de contratação. Embora possa assumir dimensão estratégica para a manutenção do processo, não há histórico disponível para sua ocorrência.	0,10
Rara	Evento casual, inesperado. Muito embora raro, há histórico de ocorrência conhecido por parte dos gestores e operadores do processo de contratação.	0,35
Eventual	Evento usual, corriqueiro. Devido à sua ocorrência habitual, seu histórico é amplamente conhecido por parte dos gestores e operadores do processo de contratação.	0,70
Frequente	Evento se reproduz muitas vezes, se repete seguidamente, de maneira assídua, numerosa e não raro de modo acelerado. Interfere de modo claro no ritmo das atividades, sendo evidente, mesmo para os que conhecem pouco o processo de contratação.	1,00

Escala de Consequências:

Impacto	Significado	Expressão
Irrelevante	Degradação na operação do processo de contratação, porém causando impactos mínimos para o órgão/entidade (em termos financeiros, danos à imagem, afetação da qualidade do processo de contratação).	10
Pouco relevante	Degradação na operação do processo de contratação, causando pequenos impactos no órgão/entidade.	20
Relevante	Interrupção do processo de contratação, causando impactos significativos para o órgão e entidade, porém passível de recuperação	50
Muito relevante	Interrupção do processo, causando impactos irreversíveis para o órgão/entidade.	100

Nível de Risco: Probabilidade X Consequências

Consequência	**Avaliação do Risco**			
Muito Relevante	Médio	Alto	Extremo	Extremo
Relevante	Baixo	Médio	Alto	Extremo
Pouco relevante	Insignificante	Baixo	Médio	Alto
Irrelevante	Insignificante	Insignificante	Baixo	Médio
	Raríssima	**Rara**	**Eventual**	**Frequente**
	Probabilidade			

Documento assinado eletronicamente por **Luciano de Oliveira Silva**, **Analista**, em 31/03/2025, às 11:13, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

Documento assinado eletronicamente por **Nelinho Teixeira Neres**, **Analista**, em 31/03/2025, às 11:15, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

Documento assinado eletronicamente por **GILSON NEDISON FERREIRA DE SOUZA**, **Gerente**, em 31/03/2025, às 11:16, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

Documento assinado eletronicamente por **AYLLA ROKXANA TRAJANO PEREIRA**, **Assessor(a)**, em 31/03/2025, às 17:43, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

Documento assinado eletronicamente por **Ana Caroline Dias Cociuffo V.**, **Assessor(a)**, em 01/04/2025, às 10:00, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **0057454896** e o código CRC **75BF5CC8**.