SERVIÇO PÚBLICO FEDERAL
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
ESTADO DE MATO GROSSO DO SUL

ESTUDO TÉCNICO PRELIMINAR – ETP

1. INFORMAÇÕES BÁSICAS

Processo nº P2026/025051-6- Formalização da Demanda

Categoria que se enquadra o ETP: SOLUÇÃO DE TIC.

2. DESCRIÇÃO DA NECESSIDADE

2.1. O Conselho Regional de Engenharia e Agronomia do Mato Grosso do Sul – Crea-MS, no desenvolvimento das suas atividades de orientar e fiscalizar, registro de pessoa física e jurídica, proporcionando para sociedade a segurança do exercício legal das profissões de Engenharia, Agronomia, Geologia, Geografia e Meteorologia, de forma eficiente e segura.

2.2. O Crea-MS possui uma infraestrutura tecnológica que armazena dados críticos de profissionais, empresas e processos de fiscalização. A interrupção ou o comprometimento desses ativos por ataques cibernéticos (como ransomwares, malwares e invasões) representa um risco direto à continuidade das atividades finalísticas da autarquia.

2.3. A atual subscrição da solução de segurança de *endpoints* está próxima do vencimento. A ausência de uma ferramenta de proteção ativa e atualizada (Antivírus e EDR) deixaria a rede do Conselho vulnerável, podendo acarretar:

a) Vazamento de dados sensíveis (em desconformidade com a LGPD);

b) Indisponibilidade dos sistemas de atendimento e fiscalização;

c) Perda de integridade das informações registradas no banco de dados;

2.4. Dessa forma, é fundamental a aquisição do referido produto, para que o Departamento de Tecnologia da Informação (DTI), continue a desempenhar de forma eficaz os trabalhos relativos ao Conselho, garantindo a continuidade das atividades pelo respectivo departamento e proporcionando melhores condições e segurança de

trabalho, visando atender às necessidades do Crea-MS.

3. ÁREAS REQUISITANTES

DTI – Departamento de Tecnologia da Informação

4. NECESSIDADES DO NEGOCIO

4.1. O Conselho Regional de Engenharia e Agronomia de Mato Grosso do Sul (Crea-MS) gere um ecossistema digital que processa diariamente ARTs (Anotações de Responsabilidade Técnica), acervos profissionais e dados sensíveis de milhares de jurisdicionados. A infraestrutura de TI é o alicerce para a fiscalização do exercício profissional em todo o Estado. Portanto, a segurança dos *endpoints* (estações de trabalho e servidores) não é um acessório, mas uma condição de existência para a operação da autarquia:

4.1.1. Contexto Institucional e Dependência Tecnológica;

4.1.2. O Problema: Exposição a Riscos Cibernéticos Elevados A atual subscrição da solução Bitdefender GravityZone possui data de expiração iminente;

4.1.3. A descontinuidade dessa proteção, ainda que por um curto período, acarreta vulnerabilidade crítica: Sem as atualizações de assinaturas e o motor de inteligência artificial (EDR), os computadores do Conselho tornam-se alvos fáceis para *exploits* de "dia zero" e malwares modernos;

4.1.4. Risco de Ransomware: O sequestro de dados paralisaria o atendimento ao público e a arrecadação, gerando prejuízo financeiro e institucional incalculável;

4.1.5. Responsabilidade Civil e Administrativa: Conforme a LGPD (Lei nº 13.709/2018), o Crea-MS tem o dever de adotar medidas de segurança aptas a proteger os dados pessoais. A ausência de antivírus atualizado configura negligência na custódia desses dados;

4.2. São funções, funcionalidades, componentes, capacidades e características que a solução deve possuir para cumprir com seu propósito e, consequentemente, atender à demanda ou resolver o problema identificado pela área requisitante. Na prática, representa o detalhamento do objeto a ser contratado, ou seja, o que a solução deve prover, independentemente da tecnologia utilizada ou dos padrões tecnológicos da instituição, é de responsabilidade do requisitante.

5. NECESSIDADES TECNOLÓGICAS

5.1. A contratação de solução de antivírus corporativo visa atender à crescente demanda por proteção dos ativos de tecnologia da informação contra ameaças cibernéticas, tais como malwares, ransomwares, phishing e ataques de dia zero, assegurando a **confidencialidade, integridade e disponibilidade das informações institucionais.**

5.2. No contexto atual do Crea-MS, identificam-se às seguintes necessidades tecnológicas:

5.2.1. Proteção avançada contra ameaças: A solução deve oferecer mecanismos de detecção e resposta baseados em múltiplas camadas, incluindo:

- Análise por assinatura e heurística;
- Inteligência artificial e machine learning;
- Proteção contra ransomware e exploits;
- Detecção de ameaças em tempo real (EDR/XDR);

5.2.2. Gestão Centralizada: Deve permitir o gerenciamento unificado de todos os *endpoints* (estações de trabalho, servidores e dispositivos móveis), com:

- Console central (preferencialmente em nuvem);

- Aplicação de políticas de segurança;
- Monitoramento em tempo real;
- Geração de relatórios e auditorias;

5.2.3. Compatibilidade e integração: A solução deve ser compatível com os ambientes da organização, incluindo:

- Sistemas operacionais (Windows, Linux, macOS);
- Integração com diretórios (ex.: Active Directory);
- Compatibilidade com outras soluções de segurança (firewall, SIEM, etc.);

5.2.4. Baixo impacto no desempenho: O antivírus deve operar com consumo otimizado de recursos, evitando degradação significativa no desempenho dos equipamentos dos usuários.

5.2.5. Atualizações automáticas e contínuas. A solução deve garantir:

- Atualizações frequentes de assinaturas e mecanismos de detecção;
- Distribuição automática e centralizada dessas atualizações;

5.2.6. Controle de dispositivos e aplicações:

- Controle de acesso a dispositivos removíveis (USB, HD externo);
- Controle de execução de aplicações (whitelisting/blacklisting);
- Proteção contra softwares não autorizados;

5.2.7. Resposta e remediação automatizada. Capacidade de:

- Isolar máquinas comprometidas;
- Remover ameaças automaticamente;
- Gerar alertas e ações corretivas em tempo real;

5.2.8. Conformidade com normas e legislações: A solução deve estar alinhada às boas práticas de segurança da informação e à legislação vigente, especialmente a Lei Geral de Proteção de Dados Pessoais, garantindo mecanismos adequados de proteção de dados pessoais.

5.2.9. Suporte Técnico e SLA:

- Suporte técnico especializado;
- Atendimento em língua portuguesa;
- Acordos de nível de serviço (SLA) compatíveis com a criticidade do ambiente;

5.2.10. Escalabilidade e flexibilidade: A solução deve permitir expansão futura, acompanhando o crescimento do parque tecnológico, sem necessidade de substituição da ferramenta.

6. DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC

6.1. A seleção da solução deverá observar, no mínimo, os seguintes requisitos:

6.1.1. Capacidade de proteção e eficácia. A solução deve demonstrar alto nível de detecção e bloqueio de ameaças, incluindo:

- Malware conhecido e desconhecido (zero-day);
- Ransomware, spyware e phishing;

- Ataques baseados em comportamento (análise heurística e comportamental);

6.1.2. Recursos de detecção e resposta (EDR/XDR):

- Detecção e resposta a incidentes;
- Investigação de eventos de segurança;
- Contenção automatizada de ameaças;

6.1.3. Gestão centralizada e visibilidade:

- Console de administração centralizada (on-premise ou em nuvem);
- Painéis (dashboards) de monitoramento;
- Relatórios detalhados e exportáveis;
- Gestão de políticas por grupos ou unidades organizacionais;

6.1.4. Facilidade de implantação e uso:

- Instalação simplificada e automatizável;
- Interface intuitiva;
- Baixa complexidade operacional;

6.1.5. Compatibilidade com o ambiente tecnológico. Deve ser compatível com:

- Sistemas operacionais utilizados (Windows, Linux, macOS);

- Infraestrutura existente (ex.: diretórios, redes, servidores);
- Ambientes virtualizados e em nuvem;

6.1.6. Impacto no desempenho dos equipamentos: Deve apresentar baixo consumo de recursos (CPU, memória e disco), garantindo a produtividade dos usuários.

6.1.7. Atualizações e inteligência de ameaças:

- Atualizações automáticas e frequentes;
- Base de inteligência global de ameaças (threat intelligence);
- Proteção em tempo real;

6.1.8. Recursos adicionais de segurança. Será considerado diferencial:

- Firewall integrado;
- Controle de dispositivos (USB, periféricos);
- Controle de aplicações (whitelisting/blacklisting);
- Proteção web e de e-mail;

6.1.9. Escalabilidade e flexibilidade. A solução deve suportar:

- Crescimento do número de *endpoints*;
- Expansão para diferentes unidades ou localidades;
- Licenciamento flexível;

6.1.10. Suporte técnico e confiabilidade do fornecedor. Deve contemplar:

- Suporte técnico especializado, preferencialmente em português;
- Tempo de resposta compatível com SLA definido;
- Histórico e reputação do fornecedor no mercado;

6.1.11. Conformidade legal e normativa: A solução deve estar aderente às normas de segurança da informação e à legislação vigente, especialmente à Lei Geral de Proteção de Dados Pessoais, garantindo proteção adequada aos dados tratados.

6.1.12. Modelo de licenciamento e custo total (TCO). A escolha deve considerar:

- Modelo de licenciamento (por dispositivo, usuário ou volume);
- Custos de implantação, suporte e manutenção;
- Relação custo-benefício ao longo do contrato;

7. ESTIMATIVA DA DEMANDA DO SERVIÇO

7.1. A demanda de aquisição do referido produto deve atender às necessidades do Crea-MS, sendo 200 (duzentas) licenças da solução por um período de 36 (trinta e seis) meses, de acordo com às configurações atuais do Crea-MS, sendo:

- *Endpoints* (Estações de Trabalho):150;
- Servidores: 50
- Caixas de e-mails: 200

7.2. As soluções devem atender os requisitos obrigatórios e recomendações, no que ser refere à aplicabilidade da Lei Geral de Proteção de Dados (LGPD). O tratamento de dados pessoais de acordo com as bases legais previstas nas hipóteses dos artigos 7º e 11º da Lei 13.709/2018;

8. LEVANTAMENTO DE SOLUÇÕES

8.1. Atualmente o Crea-MS está utilizando o antivírus Bitdefender GravityZone Business Security Premium, que vêm atendendo às expectativas do Conselho. Diante da atual utilização do produto/serviço, citamos às principais soluções equivalentes ao produto citado, disponíveis no mercado:

8.1.1. Kaspersky Endpoint Security for Business Select

- Proteção multicamada com forte foco em controle de aplicações e dispositivos;
- Recursos de EDR nas versões mais avançadas;
- Boa eficiência contra ransomware;
- Gestão centralizada (cloud ou on-premise);

8.1.2. Trend Micro Worry-Free XDR

- Plataforma com XDR (Extended Detection and Response);
- Correlação de eventos entre endpoints, e-mail e rede;
- Forte uso de inteligência de ameaças;
- Indicado para ambientes distribuídos e híbridos;

8.1.3. ESET Protect Entry 5 Device

- Baixo consumo de recursos;
- Console centralizado (ESET PROTECT);
- Boa compatibilidade com Linux;
- Evolução para EDR disponível em versões superiores;

8.1.4. Symantec Endpoint Protection Standard Requirements

- Solução tradicional e consolidada;
- Antivírus + firewall + IPS;
- Forte histórico no mercado corporativo;
- Evolução para plataforma Broadcom com recursos mais avançados;

8.1.5. Bitdefender GravityZone Business Security Premium

- Proteção multicamada com mais de 30 tecnologias baseadas em machine learning e inteligência artificial;
- Alta eficácia (até ~99,9% em testes independentes);
- Inclui EDR (Endpoint Detection and Response) com:
  I. Monitoramento contínuo;
  II. Correlação de eventos;
  III. Resposta automatizada a incidentes;
- Proteção contra:
  I. APTs (ameaças persistentes avançadas);
  II. Ransomware e exploits;
- Console centralizado (cloud ou híbrido);
- Baixo impacto de desempenho nos *endpoints*;

9. ANÁLISE COMPARATIVA DE SOLUÇÕES

9.1. Baseado nas soluções elencadas no item 8, segue abaixo quadro comparativo das soluções citadas:

Critério	Bitdefender GravityZone Premium	Kaspersky Endpoint Securit	Trend Micro XDR	ESET Protect	Symantec Endpont
Tipo	EPP + EDR	EPP + EDR	EPP + XDR	EPP(EDR opcional)	EPP
IA	Avançada	Avançada	Avançada	Moderada	Moderada
Proteção contra ransomware	Alta	Alta	Alta	Alta	Alta
Gestão centralizada	Sim (cloud/híbrido)	Sim	Sim (cloud)	Sim	Sim
Impacto em desempenho	Baixo	Médio	Médio	Baixo	Médio
Indicado para	Médio e grande porte	Médio e grande porte	Médio e grande porte	Pequeno e Médio	Médio e Grande

10. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

Não se aplica pois o mercado oferece tecnologia para atender o Serviço em questão.

11. ANÁLISE COMPARATIVA DE CUSTOS

11.1. Para subsidiar a identificação dos custos do presente Estudo Técnico Preliminar, solicitou-se proposta de preço com empresa especializada na comercialização do referido antivirus (Empresa A) e também foi realizada consulta no Portal Nacional de Contratações Públicas - PNCP (Empresas B e C), conforme quadro demonstrativo abaixo:

DESCRIÇÃO	CATSER	QT	EMPRESA A		EMPRESA B		EMPRESA C		VLOR MÉDIO UNIT	VLOR MÉDIO TOTAL
			VLR UNIT	VLR TOTAL	VLR UNIT	VLR TOTAL	VLR UNIT	VLR TOTAL		
licenciamento GravityZone Business Security Premium (36 meses)	27502	200	R$ 198,60	R$ 39.720,00	R$ 127,14	R$ 25.428,00	R$ 329,60	R$ 65.920,00	R$ 218,45	R$ 43.689,33

12. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

12.1. O levantamento de mercado evidencia à existência de múltiplas soluções maduras de antivirus corporativo, com diferentes níveis de capacidade.

12.2. Destaca-se o **Bitdefender GravityZone Business Security Premium** como uma solução de alto nível, por combinar:

- Proteção multicamada baseada em IA;
- Recursos nativos de EDR;
- Alta taxa de detecção;
- Gestão centralizada e escalável;

12.3. Dessa forma, recomenda-se que a contratação priorize soluções que contemplem, no mínimo:

- Proteção de endpoint (EPP);
- Detecção e resposta a incidentes(EDR);

13. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

13.1. Como demonstrado no quadro do item 11.1., chegamos a valor total médio de R$43.689,33 (quarenta e três mil, seiscentos e oitenta e nove reais e trinta e três centavos) para aquisição de 200 (duzentas) licenças de antivírus no período de 36 (trinta e seis) meses.

14. JUSTIFICATIVA TÉCNICA DA ESCOLHA DA SOLUÇÃO

14.1. A presente justificativa tem por finalidade fundamentar a escolha da solução de antivírus corporativo a ser adotada pela Administração, com base no levantamento de mercado realizado e na análise comparativa das alternativas disponíveis.

14.2. O cenário atual de segurança da informação evidencia o aumento significativo de ameaças cibernéticas, especialmente aquelas direcionadas a ambientes corporativos, tais como ransomware, ataques de dia zero e ameaças persistentes avançadas (APT). Nesse

contexto, soluções tradicionais de antivírus (EPP) mostram-se insuficientes para garantir a adequada proteção dos ativos de tecnologia da informação, sendo necessária a adoção de ferramentas mais robustas, que integrem capacidades de **detecção e resposta a incidentes (EDR)** e, preferencialmente, mecanismos avançados de análise comportamental e inteligência artificial.

14.3. O levantamento de mercado identificou diversas soluções consolidadas, tais como Kaspersky Endpoint Security for Business, Trend Micro Worry-Free XDR, ESET PROTECT e Symantec Endpoint Protection, todas com funcionalidades relevantes e ampla adoção no mercado. Contudo, observou-se que tais soluções apresentam variações quanto ao nível de maturidade, integração de recursos avançados e capacidade de resposta automatizada.

14.4. Dentre as soluções analisadas, destaca-se o Bitdefender GravityZone Business Security Premium, que se posiciona como solução de nível avançado (EPP + EDR), apresentando diferenciais técnicos relevantes, tais como:

- Utilização de múltiplas camadas de proteção baseadas em inteligência artificial e machine learning, proporcionando elevada taxa de detecção de ameaças conhecidas e desconhecidas;
- Recursos nativos de EDR, permitindo monitoramento contínuo, correlação de eventos e resposta automatizada a incidentes de segurança;
- Capacidade de proteção contra ameaças sofisticadas, incluindo ransomware, exploits e ataques direcionados;
- Console de gerenciamento centralizado, com possibilidade de operação em nuvem ou ambiente híbrido, facilitando a administração e o controle dos endpoints;
- Baixo impacto no desempenho dos equipamentos, fator essencial para não comprometer a produtividade dos usuários;
- Escalabilidade e aderência a ambientes corporativos de médio e grande porte;

14.5. Adicionalmente, a solução encontra-se alinhada às boas práticas de segurança da informação e às exigências legais vigentes, especialmente à Lei Geral de Proteção de Dados Pessoais, contribuindo para a proteção adequada dos dados pessoais tratados pela

Administração.

14.6. Importa destacar que, embora existam outras soluções com características semelhantes, o **Bitdefender GravityZone Business Security Premium** apresenta melhor equilíbrio entre nível de proteção, recursos avançados integrados (sem necessidade de módulos adicionais), facilidade de gestão e custo-benefício, mostrando-se tecnicamente mais vantajoso para atendimento das necessidades institucionais.

14.7. Dessa forma, conclui-se que a adoção de solução que atenda, no mínimo, às características técnicas equivalentes ou superiores ao Bitdefender GravityZone Business Security Premium mostra-se a alternativa mais adequada para garantir a segurança dos ativos de informação, a continuidade dos serviços e a mitigação de riscos cibernéticos no âmbito da Administração Pública.

15. JUSTIFICATIVA ECONÔMICA DA ESCOLHA DA SOLUÇÃO

15.1. Continuar utilizando o antivírus Bitdefender GravityZone Business, justifica-se pela renovação por eficiência e padronização à necessidade do negócio, focando na continuidade operacional (conforme a Portaria Crea-MS nº 039/2024).

15.2. A opção pela renovação da solução já implantada justifica-se pelos seguintes fatores de eficiência:

15.2.1. Eliminação de Custo de Troca (Switching Cost): A migração para um novo fabricante exigiria a desinstalação e instalação de agentes em toda a rede corporativa, com riscos de conflitos de sistema e indisponibilidade temporária;

15.2.2. Aproveitamento de capital intelectual: A equipe técnica do Crea-MS já possui domínio sobre o console de gestão centralizada do Bitdefender, não sendo necessário novo investimento em tempo e dinheiro para capacitação;

15.2.3. Histórico de Estabilidade: A solução atual apresenta desempenho técnico satisfatório, com baixo consumo de recursos de hardware e alta taxa de detecção, já estando homologada no ambiente de produção do Crea-MS;

15.2.4. Alinhamento com o interesse público a contratação visa assegurar que os

serviços prestados aos profissionais e empresas do sistema Confea/Creas não sofram interrupções por incidentes de segurança, garantindo a integridade do patrimônio público digital e a confiança da sociedade nas bases de dados do Crea-MS.

16. BENEFÍCIOS A SEREM ALÇANÇADOS COM A AQUISIÇÃO DOS SOFTWARES

16.1. A aquisição de solução de antivírus corporativo visa proporcionar ganhos significativos à Administração, especialmente no que se refere à segurança da informação, continuidade dos serviços e conformidade legal. Dentre os principais benefícios esperados, destacam-se:

16.1.1. Elevação do nível de segurança da informação:

- A implementação da solução permitirá a proteção efetiva dos ativos tecnológicos contra ameaças cibernéticas, como malwares, ransomwares, phishing e ataques de dia zero, reduzindo significativamente a superfície de ataque e os riscos de comprometimento dos sistemas institucionais.

16.1.2. Prevenção e mitigação de incidentes de segurança:

- Com o uso de tecnologias avançadas, como análise comportamental e mecanismos de detecção e resposta (EDR), será possível identificar e neutralizar ameaças de forma proativa, minimizando impactos operacionais e financeiros decorrentes de incidentes.

16.1.3. Garantia da continuidade dos serviços:

- A proteção dos endpoints contribui diretamente para a

manutenção da disponibilidade dos sistemas e serviços prestados pela Administração, evitando interrupções causadas por ataques cibernéticos ou infecções generalizadas.

16.1.4. Gestão centralizada e maior controle do ambiente:

- A adoção de uma solução corporativa permitirá o gerenciamento centralizado de todos os dispositivos, com aplicação de políticas de segurança, monitoramento em tempo real e geração de relatórios, aumentando a visibilidade e o controle sobre o ambiente de TI.

16.1.5. Aumento da produtividade dos usuários:

- Ao reduzir ocorrências de infecção, lentidão e indisponibilidade dos equipamentos, a solução contribui para a melhoria da experiência do usuário e para a continuidade das atividades laborais sem interrupções indevidas.

16.1.6. Conformidade com normas e legislações vigentes:

- A solução auxiliará no atendimento às boas práticas de segurança da informação e à legislação aplicável, especialmente à Lei Geral de Proteção de Dados Pessoais, mitigando riscos de sanções administrativas e danos à imagem institucional.

16.1.7. Redução de custos com incidentes e suporte técnico:

- A prevenção de ataques e a automação de respostas a incidentes

reduzem a necessidade de intervenções corretivas, retrabalho e custos associados à recuperação de sistemas e dados comprometidos.

16.1.8. Escalabilidade e adaptação ao crescimento institucional:

- A solução permitirá a expansão do ambiente protegido de forma estruturada, acompanhando o crescimento do parque tecnológico da instituição sem perda de eficiência ou necessidade de substituição da ferramenta.

16.1.9. Melhoria na capacidade e auditoria e tomada de decisão:

- Com relatórios detalhados e históricos de eventos de segurança, a Administração terá subsídios para auditorias, prestação de contas e tomada de decisões estratégicas relacionadas à segurança da informação.

17. PROVIDÊNCIAS A SEREM ADOTADAS

Considerando que a pretensa aquisição se assemelha ao rol de aquisições já efetuadas no âmbito do Crea-MS, o Conselho dispõe de empregados indicados para fiscalização e gestão contratual, os quais possuem ampla experiência em suas respectivas áreas de atribuição, bem como já participaram de capacitações nesta área. Neste sentido, não se faz necessário adoção de providências prévias à celebração do contrato para sua implantação.

18. DECLARAÇÃO DE VIABILIDADE

Declaro viável a renovação da solução antivírus Bitdefender GravityZone Business, representando um investimento essencial para a proteção dos ativos de informação da Administração Pública, proporcionando maior segurança, eficiência operacional e aderência às

exigências legais, além de contribuir para a sustentabilidade e confiabilidade dos serviços prestados pelo Crea-MS para os profissionais e empresas do sistema Confea/Creas, bem como para a sociedade em geral

Justificativa da Viabilidade:

O presente Estudo Técnico Preliminar foi elaborado em conformidade com o disposto na Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, considerando o atendimento as necessidades da contratação elencadas pela Área Requisitantes bem como, seus potenciais benefícios em termos de eficácia, eficiência, efetividade e economicidade para a Administração Pública

19. RESPONSÁVEL(IS)

Responsável pela Formalização da Demanda:

Nilton João Xavier Sanches
Analista de TI

Aprovação:

João André Zago Sobrinho
Gerente de Departamento de Tecnologia da Informação

Documento assinado eletronicamente por **Nilton João Xavier Sanches**, **Analista de Sistemas,** em **24/04/2026**, às **13:02**, conforme horário oficial de Campo Grande, com fundamento no art. 4º, § 3º, do DECRETO Nº 10.543, DE 13 DE NOVEMBRO DE 2020

Documento assinado eletronicamente por **João André Zago Sobrinho**, **Gerente,** em **24/04/2026**, às **13:03**, conforme horário oficial de Campo Grande, com fundamento no art. 4º, § 3º, do DECRETO Nº 10.543, DE 13 DE NOVEMBRO DE 2020