

MJ-DPRF-DEPART.DE POL.RODOVIARIA FEDERAL/DF

Estudo Técnico Preliminar 70/2025

1. Informações Básicas

Número do processo: 08650.032146/2025-38

2. Descrição da necessidade

2.1. A Polícia Rodoviária Federal (PRF) atua em uma área estratégica e sensível da segurança pública, estando constantemente exposta a diversos riscos tecnológicos que podem comprometer a integridade, confidencialidade e disponibilidade das informações institucionais. Considerando o aumento crescente e constante das ameaças cibernéticas, torna-se imprescindível garantir a proteção dos equipamentos de informática, tais como notebooks e estações de trabalho utilizados pelos agentes que atuam nas atividades operacionais e administrativas, além da rede atualmente implantada.

2.2. O ambiente tecnológico do órgão está diariamente suscetível a ataques como: malwares, ransomwares, vírus, tentativas de invasão e outras ameaças digitais que podem comprometer operações, sigilo de dados sensíveis e a continuidade dos serviços prestados pela PRF. Essas ameaças podem comprometer a confidencialidade, integridade e disponibilidade das informações institucionais, causando impactos severos como a perda de dados sensíveis, interrupção das operações, danos à reputação da instituição e, em casos extremos, a paralisação temporária ou permanente de sistemas críticos para a segurança pública. Dada a natureza estratégica das informações manuseadas pela PRF — incluindo dados pessoais, informações sigilosas de investigações, controle de operações táticas e monitoramento de ocorrências — a proteção contra tais ameaças não pode ser apenas uma medida acessória, mas uma prioridade estratégica.

2.3. Adicionalmente, a PRF está sujeita a um conjunto rigoroso de normas e regulamentações, relacionadas à segurança da informação e proteção de dados, como a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), a Política Nacional de Segurança da Informação (PNSI), além das diretrizes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), que exigem a implementação de mecanismos de defesa adequados para assegurar a conformidade legal e a integridade dos sistemas institucionais.

2.4. Nesse contexto, a obtenção da solução de antivírus de última geração é fundamental para mitigar vulnerabilidades tecnológicas e fortalecer a postura de segurança cibernética do órgão. A solução deverá oferecer proteção abrangente contra ameaças conhecidas e emergentes, utilizando técnicas avançadas e atualizações contínuas em tempo real para garantir resiliência contra ameaças em constante evolução.

2.5. Segundo dados do Centro de Proteção, Tratamento e Resposta a Incidentes Cibernéticos do Governo - CTIR Gov, os órgãos governamentais brasileiros têm enfrentado uma crescente onda de ataques cibernéticos. No primeiro trimestre de 2025, foram registrados 2.356 incidentes digitais em instituições públicas nacionais, sendo 1.748 relacionados a vazamentos de dados. Esse número alarmante reflete uma tendência de alta que já vinha se consolidando nos anos anteriores. Em 2024, por exemplo, o Governo Federal contabilizou 7.474 vazamentos de dados ao longo do ano, mais que o triplo dos 1.615 casos ocorridos entre 2020 e 2023. Esses dados ilustram claramente que as instituições públicas se tornaram alvos preferenciais de atores maliciosos, exigindo atenção redobrada e investimentos em segurança cibernética.

2.6. Atualmente a Polícia Rodoviária Federal possui a Coordenação de Integração, Segurança e Ciência de Dados que gerencia o atual contrato vigente nº 01/2022 - Doc. SEI Nº 38368692, no qual se contempla o licenciamento, implantação, suporte técnico, capacitação, garantia e atualização de uma Plataforma de Proteção de Endpoint (EPP),

Solução de Detecção e Resposta a Incidentes (EDR) e Solução Contra Ameaças Persistentes Avançadas (APT), abrangendo a Sede Nacional, as Unidades Regionais e a Universidade Corporativa da PRF, cuja vigência irá ser expirada 03/04/2026.

2.7. Considerando a complexidade e a criticidade dos serviços prestados, bem como a necessidade de garantir a continuidade da proteção cibernética institucional, torna-se necessário iniciar, de forma planejada, os estudos técnicos que subsidiarão o escopo da melhor solução que possa atender a instituição. Tal medida busca evitar descontinuidade dos serviços, mitigar riscos de segurança da informação e assegurar a prestação dos serviços públicos prestados pela Polícia Rodoviária Federal.

3. Área requisitante

Área Requisitante	Responsável
Coordenação de Infraestrutura, Segurança e Ciência de Dados	Fábio Cova Martins

4. Necessidades de Negócio

4.1 Elencam-se as seguintes necessidades de negócio, conforme abaixo:

NECESSIDADES DE NEGÓCIO	
1	<p>Gerenciar a transição contratual</p> <ul style="list-style-type: none">• Substituição do objeto do Contrato Administrativo nº 1/2022 (SEI Nº 38368692), processo SEI Nº 08650.035516/2021-65 e Contrato Administrativo nº 5/2021 (SEI Nº 30839008), processo SEI Nº 08650.004135/2019-10, com o objetivo de prover mais segurança com o aumento da capacidade de detecção, análise e resposta em tempo hábil a ameaças mais avançadas, visando proteger a rede da PRF contra vazamentos de dados sigilosos e comprometimento da disponibilidade de sistemas críticos hospedados;
2	<p>Garantir a continuidade operacional da instituição</p> <ul style="list-style-type: none">• Proteger os sistemas e estações de trabalho contra indisponibilidades causadas por vírus, ransomware, trojans ou outras formas de malware que possam comprometer os serviços essenciais da PRF.• Evitar interrupções em sistemas de missão crítica (como comunicações, acesso a bases de dados integradas com outros órgãos, registros operacionais, etc.).
3	<p>Proteger dados sensíveis e informações institucionais</p> <ul style="list-style-type: none">• Evitar vazamentos de dados pessoais, corporativos ou estratégicos da PRF.• Atender à LGPD (Lei Geral de Proteção de Dados) e outras legislações de proteção de dados.• Proteger informações classificadas ou sensíveis, como operações policiais, inteligência, etc.

4	<p>Detectar e responder a ameaças avançadas</p> <ul style="list-style-type: none"> • Aumentar a capacidade da PRF de detectar ameaças que ultrapassam antivírus tradicionais, como APTs (Ameaças Persistentes Avançadas), exploits de dia zero, fileless malware, etc. • Monitorar, rastrear e responder a comportamentos suspeitos em tempo real por meio de soluções EDR integradas.
5	<p>Reduzir riscos reputacionais e institucionais</p> <ul style="list-style-type: none"> • Proteger a imagem institucional da PRF diante de possíveis incidentes de segurança, como vazamentos ou paralisação de sistemas. • Evitar exposição negativa na mídia, responsabilizações administrativas ou judiciais.
6	<p>Atender a requisitos de governança e auditoria</p> <ul style="list-style-type: none"> • Ter visibilidade centralizada e auditável sobre os eventos de segurança em endpoints. • Gerar relatórios e evidências para inspeções, CGU, TCU e auditorias internas. • Permitir rastreabilidade de incidentes, apoio à forense digital e conformidade com controles de segurança da informação (ex: ISO 27001/27701, NIST, COBIT, etc.).
7	<p>Capacitar a instituição para lidar com ameaças futuras</p> <ul style="list-style-type: none"> • Atualizar as defesas cibernéticas com soluções modernas e em conformidade com as melhores práticas do mercado. • Fornecer ao time técnico ferramentas adequadas para prevenção, detecção e resposta a incidentes.
8	<p>Cobrir todas as unidades da PRF em nível nacional</p> <ul style="list-style-type: none"> • Assegurar proteção homogênea para a Sede Nacional, Unidades Regionais e Universidade Corporativa, incluindo computadores, notebooks e outros endpoints que acessem a rede institucional. • Permitir gestão centralizada, mesmo em ambientes distribuídos geograficamente.
9	<p>Atualização contínua e suporte especializado</p> <ul style="list-style-type: none"> • Garantir que a solução seja atualizada automaticamente com as últimas definições de ameaças. • Ter acesso a suporte técnico especializado para resolução de problemas críticos.

5. Necessidades Tecnológicas

5.1 Elencam-se as seguintes necessidades tecnológicas, conforme abaixo:

NECESSIDADES TECNOLÓGICAS

1	A solução endpoint deve ser fornecida para proteção de 11.182 (onze mil e cento e oitenta e dois) estações de trabalho e servidores;
2	A solução deverá detectar e bloquear conteúdo malicioso em tempo real através de download da internet ou através de arquivos copiados de pendrive nos computadores de usuários;
3	A solução de segurança contra ameaças persistentes e avançadas deverá prover proteção a estações de trabalho (Endpoint) no combate a códigos maliciosos (Malwares) e técnicas de exploração de vulnerabilidades de aplicações (Exploits) conhecidas e desconhecidas, chamadas de dia zero.
4	A solução deve monitorar e gerir riscos que permitam a identificação de ameaças digitais conhecidas e não conhecidas por soluções de antivírus tradicionais, permitindo a composição de serviços de mitigação complementares para a segurança do ambiente.
5	A solução deve apresentar, por meio de console centralizado, estatísticas das ameaças, sendo ela responsável pelos relatórios apontando fonte de infecção na rede monitorada e os ataques que foram direcionados aos computadores de usuários
6	A solução deverá prover uma console de gerenciamento unificada em interface gráfica WEB segura, utilizando o protocolo HTTPS ou console do próprio fabricante;
7	Implementar através da interface gráfica, seleção dos níveis e módulos de geração de log, tais como: log de autenticação, log de falhas de hardware, log de eventos de sistema, log de atualização e log de mudança de configuração.
8	Implementar solução de segurança para proteção de aplicações, servidores físicos, virtuais e container.
9	Fornecer visibilidade contínua, avaliação de riscos e priorização de ações para a superfície de ataque em ambientes de nuvem. Ele capacita as organizações a identificar, analisar e mitigar proativamente os riscos cibernéticos associados aos seus ativos e configurações na nuvem.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

6.1. Capacitação

6.1.1. A presente solução não requer capacitação técnica para a execução contratual.

6.2. Requisitos legais

6.2.1. A presente instrução deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis;

6.2.2. Lei Complementar 123, de 14 de dezembro de 2006. Institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte;

6.2.3. Decreto nº 7.174, de 12 de maio de 2010. Regulamenta a contratação de bens e serviços de informática e automação pela Administração Pública federal (no que não contrariar a Lei nº 14.133/2021);

6.2.4. Decreto nº 8.538, de 06 de outubro de 2015. Regulamenta o tratamento favorecido, diferenciado e simplificado para as microempresas e empresas de pequeno porte (no que não contrariar a Lei nº 14.133/2021);

6.3. Requisitos de Manutenção

6.3.1. Devido às características da solução, há necessidade de realização de manutenções corretivas, preventivas, adaptativa e evolutiva pela Contratada, visando à manutenção da disponibilidade da solução e ao aperfeiçoamento de suas funcionalidades;

6.3.2. O referido serviço deverá fornecer suporte corporativo telefônico, on-line ou e-mail, em português do Brasil, sem custo adicional, ilimitado, durante o período de contrato estendido ao período de garantia, todos os dias da semana, 24 horas por dia, sem limite de chamados.

6.3.3. Deverá ser disponibilizado sistema de atendimento via web com capacidade para registrar e acompanhar os chamados técnicos.

6.4. Requisitos Temporais

6.4.1. O início da implantação da solução deverá ocorrer em até 5 (cinco) dias corridos após a emissão da Ordem de Serviço.

6.4.2. A futura CONTRATADA deverá apresentar, para aprovação da CONTRATANTE, no prazo máximo de 10 (dez) dias corridos, contados a partir da data de assinatura do Contrato, o Plano de Implantação da solução contendo cronograma detalhado de atividades a serem executadas pela CONTRATADA e pela CONTRATANTE.

6.4.3. A CONTRATANTE terá até 5 (cinco) dias corridos para aprovar o Plano de Implantação.

6.4.4. Caso o Plano de Implantação apresentado não seja aprovado, a CONTRATADA terá 3 (três) dias corridos para reformular o Plano de Implantação de acordo com as exigências da CONTRATANTE.

6.4.4.1. A CONTRATANTE terá até 5 (cinco) dias corridos para aprovar o Plano de Implantação reformulado.

6.4.5. O Plano de Implantação deve conter no mínimo as seguintes informações:

6.4.5.1. Cronograma detalhado ao nível de atividades a serem desenvolvidas para a implantação da solução prevista no Termo de Referência;

6.4.5.2. Identificação de cada item da solução e modelos a serem utilizados, além do pessoal envolvido na execução dos serviços.

6.4.6. A implantação da solução deverá ser executada a partir da Divisão de Segurança da Informação e Comunicação, no Edifício-Sede do Departamento de Polícia Rodoviária Federal, situado no Setor Policial Sul, Quadra 3, Lote 5, Brasília/DF, CEP 70.610-909, e-mail: cisc@prf.gov.br, no horário comercial compreendido entre 08:00 e 18:00h.

6.4.6.1. Para a implementação da solução de APT, deverá ser implantada a solução de DDI de 1 Gbps (virtual appliance) nas regionais MG, PR, RJ e UNIPRF. Caso haja necessidade técnica para a conclusão das etapas de configuração e integração que não possam ser realizadas remotamente, a CONTRATADA deverá realizar o atendimento presencial nestas unidades, sem ônus adicional.

6.4.7. A implantação completa da solução, compreendendo todos os itens e etapas previstas no Termo de Referência, deverá ser concluída em até 60 (sessenta) dias corridos, contados da emissão da Ordem de Serviço.

6.5. Requisitos de segurança e privacidade

6.5.1. A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação do Contratante;

6.5.2. A CONTRATADA deverá manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse da PRF de que tomar conhecimento em razão da execução do Contrato.

6.5.3. Para formalização da confidencialidade exigida, a Contratada deve assinar TERMO DE COMPROMISSO MANUTENÇÃO DE CONFIDENCIALIDADE — TCMC-PJ, comprometendo-se a respeitar todas as obrigações relacionadas com confidencialidade e segurança das informações pertencentes à Contratante, mediante ações ou omissões, intencionais ou acidentais, que impliquem na divulgação, perda, destruição, inserção, cópia, acesso ou alterações indevidas, independentemente do meio no qual estejam armazenadas, em que trafeguem ou do ambiente em que estejam sendo processadas.

6.5.4. O Termo de Confidencialidade abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao Contrato, a que diretamente ou pelos seus empregados, a Contratada venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do Contrato.

6.5.5. A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do Contrato sobre a existência do Termo de Confidencialidade, bem como da natureza sigilosa das informações.

6.5.6. A quebra da confidencialidade e/ou do sigilo das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislação em vigor, podendo até culminar na rescisão do contrato.

6.5.7. Observar, no que couber, a versão mais recente do "Guia de Requisitos e de Obrigações quanto a Segurança da Informação e Privacidade", de autoria Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos. Guia disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/framework-guias-e-modelos>

6.6. Subcontratação

6.6.1. Será vedada a subcontratação.

6.6.2. A subcontratação dilui a responsabilidade. Se houver um incidente de segurança, uma falha na atualização ou um vazamento de dados, a administração poderia enfrentar dificuldades para determinar a quem responsabilizar: a contratada principal ou a subcontratada. Ao proibir a subcontratação, a administração garante que o fornecedor principal seja o único ponto de contato e o único responsável por todas as obrigações contratuais, inclusive a conformidade com as leis de proteção de dados.

6.6.3. Ainda no tocante à segurança da informação, soluções de segurança de TIC lidam com dados altamente sensíveis, incluindo informações sobre vulnerabilidades da rede, tentativas de ataques e dados pessoais de usuários. A empresa contratada tem acesso privilegiado a informações críticas da infraestrutura do órgão público.

6.6.4. A subcontratação introduz um novo ator, com acesso a essa infraestrutura. Isso aumenta o risco de segurança, pois a administração não tem controle sobre os processos, políticas de segurança ou a confiabilidade da empresa subcontratada. Vetar a subcontratação é uma medida de controle de acesso, que limita o número de entidades com acesso à rede e garante que apenas a empresa que passou pelo rigoroso processo de qualificação da licitação tenha acesso a informações sensíveis.

7. Estimativa da demanda - quantidade de bens e serviços

7.1. Diante das informações citadas, mediante estudos técnicos realizados dentro da Coordenação especialista, chegou-se a seguinte estimativa das quantidades dos itens necessários, ao atendimento da necessidade do órgão:

Item	Descrição	unidade	Quantidade Mínima ao ano	Quantidade Máxima ao ano
1	Solução de EPP (Plataforma de proteção de endpoint): solução implantada em dispositivos endpoint para evitar ataques de malware baseados em arquivos, detectar atividades maliciosas e fornecer os recursos de investigação e correção necessários para responder a incidentes e alertas de segurança dinâmicos, incluindo software, gerenciamento centralizado, licenciamento, suporte técnico e garantia pelo período contratual.	Host	11.182	24.682
2	Créditos para utilização de sandbox (ambiente isolado para análise malware) cujo o escopo devem ser os pilares: Análise, Desempenho e Integração. A solução deve oferecer uma capacidade robusta de emulação de múltiplos sistemas operacionais e ser capaz de detectar ameaças que usam técnicas de evasão, fornecendo um relatório forense detalhado e acionável com base no comportamento do arquivo.	Unitário	225.000	450.000
	Solução de APT			

3	<p>(Proteção Contra Ameaças Persistentes Avançadas): solução de monitoramento contínuo que oferece visibilidade em tempo real, contra ameaças avançadas, como exploits de zero-day e malwares personalizados, que se caracterizam por serem desconhecidas, direcionadas e evasivas, tornando ineficientes as ferramentas de antivírus baseadas apenas em assinaturas para detecção de conteúdo malicioso, incluindo software, gerenciamento centralizado, licenciamento, suporte técnico e garantia pelo período contratual.</p>	Volume Mínimo de Dados	8 Gbps	12 Gbps
4	<p>Solução de EDR (detecção e resposta a ameaças): Solução de monitoramento e resposta contínuos a ameaças avançadas de segurança cibernética, incluindo software, gerenciamento centralizado, licenciamento, suporte técnico e garantia pelo período contratual.</p>	Host	300	750
5	<p>Solução de gerenciamento de riscos em ambiente de nuvem. Ter capacidade de atuar de forma proativamente na identificação de riscos em todos os seus ativos de rede da PRF disponibilizados nas Nuvem AWS, GCP, Azure, Huawei Cloud, IBM Cloud e Oracle Cloud.</p>	Ativos	3	6

6	Serviço de Suporte	Meses	12	12
7	Serviço de Instalação de solução de proteção contra ameaças persistentes avançadas (Solução Anti-apt)	Serviço	0	4

7.2. Foi utilizada a seguinte memória de cálculo para se chegar às quantidades expostas acima:

7.2.1 O item número nº 01 - Plataforma de proteção de endpoint foi calculado, com base na média de dispositivos, oriundos de consulta a informações do patrimônio e pesquisa do parque de TI, junto à Coordenação de infraestrutura, chegando-se a um mapeamento dos ativos que precisam ser protegidos no ambiente da PRF:

Tipo de equipamento/estação	estimativa
Notebook/Desktops (A):	10.377
Servidores físicos e virtuais (infra geral) (B):	300
Reserva Técnica Rotativa Notebooks/Desktops (C):	505
Total (A+B+C):	11.182

7.2.2. Com base em estudos feitos pela equipe de Gerenciamento de projetos em TI, considerando que o contrato poderá se estender por 60 meses, criou-se uma projeção de crescimento da necessidade em **120,73%** na quantidade de hosts, estimando assim um volume máximo de 24. 682 hosts, ao ano, para permitir a instalação nos aparelhos mobiles distribuídos para cada policial, que utilizam o aparelho para acesso aos sistemas principais do órgão;

7.2.3. Essa prática de estimar quantidades mínimas e máximas para itens como *hosts* em uma solução de segurança corporativa, é uma prática comum no mercado, que serve para propósitos comerciais, técnicos e operacionais.

7.2.3.1. A maioria das soluções de segurança atualmente no mercado é licenciada por dispositivo (host), por usuário, ou por volume de dados. Como ambientes de TI mudam o tempo todo (entra e sai máquina, criam-se projetos novos, aumenta-se escopos de trabalho), é comum:

a) Ter uma previsão mínima (o que já se sabe que será necessário).

b) E uma previsão máxima (o teto que você pode atingir com expansão, crescimento ou picos temporários).

7.3. Em relação ao item número nº 02 - créditos para utilização de Sandbox, primeiramente esclarece-se que a sandbox é um ambiente isolado e seguro onde arquivos, URLs, scripts ou executáveis suspeitos são executados para análise. Serve para detectar malwares avançados, ransomwares, exploits ou ameaças que poderiam passar despercebidos em uma verificação tradicional.

7.3.1. Nas soluções do gênero de segurança cibernética, o uso da sandbox geralmente consome "créditos". Cada crédito representa uma análise sandbox de um item (um arquivo, uma URL suspeita, um anexo de e-mail).

7.3.2. Assim, o volume anual de análises sandbox é feito com base no número de dispositivos ativos, frequência de análise e tipo de itens analisados.

7.3.3. Dessa forma, foi feita a seguinte análise:

--	--

Variáveis	Quantidade estimada
Número de hosts protegidos	11.182
Proporção de hosts que geram eventos analisáveis	56% (6.261)
Eventos com potencial de análise sandbox por mês	média de 3 eventos por host por mês
Total mensal de análises	$6.261 \times 3 = 18.783$
Total anual de análises (créditos) (mínima)	$18.783 \times 12 =$ aproximadamente 225.000
Total anual de análises (créditos) (máxima), levando em consideração ao aumento em 100% do número de ativos (para permitir a instalação nos aparelhos mobiles distribuídos para cada policial, que utilizam o aparelho para acesso aos sistemas principais do órgão).	aproximadamente 450.000

7.4. Em relação ao item nº 03 - Uma solução de APT (Proteção Contra Ameaças Persistentes) é uma solução voltada para detecção de ameaças na rede. Ele atua como um sensor de tráfego, monitorando e inspecionando tudo que passa pela rede, em tempo real. O DDI não é licenciado por dispositivo, como um antivírus tradicional. Ele é mensurado por capacidade de tráfego de rede que consegue monitorar.

7.4.1. Dessa forma devido à estrutura da Polícia Rodoviária federal, chega-se à seguinte memória de cálculo da quantidade necessária:

ESTIMATIVA DO TRÁFEGO MONITORADO	
Segmento/local	Tráfego médio estimado (Mbps)
Sede nacional (DF)	2.400 Mbps
Superintendências regionais e UNIPRF (28)	$100 \text{ Mbps} \times 28 =$ 2.800 Mbps
Unidades operacionais e postos	1.000 Mbps (consolidados)
Sistemas em nuvem e integração externa	1.800 Mbps

Total estimado (mínimo)	8.000 Mbps (ou 8 Gbps)
Total estimado (máximo), em caso de haver um incremento de 50 % no tráfego	12.000 Mbps (ou 12 Gbps)

7.4.2. Para a solução de APT- Proteção Contra Ameaças Persistentes Avançadas, a necessidade é a expansão da proteção para as demais unidades descentralizadas do órgão, que por terem relação de confiança entre os ativos de segurança, precisam ser dotadas das mesmas proteções implementadas na sede, devendo ser implementada a solução de DDI de 1gbps (*virtual appliance*) em cada uma das seguintes regionais (MG, PR e RJ) e na Universidade Corporativa da Polícia Rodoviária Federal, devido ao volume de dados e tipos de serviços realizados por essas unidades descentralizadas.

7.5. Em relação ao item nº 04 - Solução de EDR (detecção e resposta a ameaças), trata-se de uma plataforma mais avançada, que a equipe técnica vislumbrou para o monitoramento de ambientes mais críticos, conforme apontado abaixo:

Categoria de Equipamento	Quantidade Estimada	Observações
Servidores de aplicação e banco de dados	100	Hospedam sistemas de controle, bancos de dados sensíveis.
Estações críticas em centros de comando e controle	80	Operações táticas, análise de vídeo e inteligência.
Máquinas virtuais em nuvem (AWS, Azure, GovCloud)	70	VMs para serviços administrativos e operacionais
Terminais de alta segurança (inteligência e corregedoria)	50	Equipamentos com dados altamente sensíveis
Total (mínimo)		300 Host
Total (máximo, considerando uma expansão de 150 %		750 Host

7.5.1. Para a solução para proteção de aplicações, servidores físicos, virtuais e container, a necessidade do incremento de licenças, justifica-se pelo aumento da cobertura dos servidores, nos ambiente de produção, homologação e desenvolvimento, totalizando atualmente 750 servidores (físicos e virtuais).

7.6. O item nº 05 - Solução de gerenciamento de riscos em ambiente de nuvem, é uma ferramenta capaz de mapear, identificar e monitorar a superfície de ataque de uma organização — especialmente recursos expostos na nuvem ou na internet. Como a PRF possui sistema em nuvem e rede distribuída é necessário a realização de verificações periódicas, sendo estrategicamente indicado um monitoramento a cada 4 meses da superfície de ataque, conforme abaixo:

Fator considerado	Justificativa técnica
Número de unidades regionais (28)	Ambientes descentralizados com variações regionais.
Ambientes em nuvem e híbridos em constante evolução	Aumento no uso de nuvem (GovCloud, AWS, GCP, Azure, Huawei Cloud, IBM Cloud e Oracle Cloud), com novos serviços e API.
Mudanças operacionais frequentes	Publicações de novos sistemas, mudanças em domínios, acessos externos.
Risco de exposição acidental	Ex: Bucket S3 aberto, portas expostas, serviços mal configurados.
Conformidade com políticas de segurança	Estabelecimento de varreduras periódicas como política de gestão de risco.
Custo-benefício	3 varreduras/ano evitam licenciamento mensal contínuo, mas ainda garantem controle. Em caso de aumento da necessidade foi estipulado um percentual máximo de recrudescimento em 100%, ou seja 6.

7.7. O item nº 06 - **de Suporte**, foi feita a estimativa de 12 unidades ao ano, a fim de ter disponibilidade mensal, em caso de necessidade de manutenções pontuais.

7.8. O item nº 07 - Serviço de Instalação da Solução de Proteção Contra Ameaças Persistentes Avançadas, que é a atividade profissional de instalação e configuração do sensor do módulo APT, que é uma solução de detecção de ameaças em rede (network sensor), por se tratar de um evento mais pontual e específico, estimou-se como mínimo a quantidade de 0, e máximo a quantidade 4. O porquê, parte do pressuposto de que nenhum novo sensor está precisando de instalação imediata. O número 4, reflete a possível expansão para até 4 novas localidades prioritárias, como:

- a) Sede nacional (DF).
- b) Regiões com maior tráfego de dados ou risco.
- c) Pontos de integração com redes externas.

7.9. Verificou-se que não há solução que atenda à necessidade deste processo de contratação no Catálogo de Soluções de TIC com condições padronizadas para licenciamento de software. Desta forma, não há de se considerar o PMC-TIC.

7.10. Todo dimensionamento apontado acima, baseou-se no parque que consta com:

- 7.10.1. Sistemas Operacionais diversos: Windows Server (2008, 2012, 2016, 2019), Oracle Linux e Linux RedHat;
- 7.10.2. Bancos de Dados variados: SQL Server, Postgres, Informix, MySQL, MongoDB e Oracle;
- 7.10.3. Ambiente do Usuário com Sistema Operacional: Windows 10, 11, MacOS e Linux;
- 7.10.4. Utilitários e Aplicativos: Plataforma Google Workspace, MS Office, Libre Office, Acrobat Reader e Antivírus TrendMicro.
- 7.10.5. Ambientes em Nuvem: Azure, AWS (Amazon Web Services), Google Cloud Platform (GCP), Huawei Cloud, IBM Cloud e Oracle Cloud.

7.11. Quantidades mínimas a serem contratadas (Adequação Orçamentária)

- 7.11.1. A presente contratação foi estruturada para permitir que a PRF adquira o quantitativo integral de todos os itens licitados — incluindo licenciamento de endpoints, créditos de sandbox, capacidade de tráfego de rede (Gbps), monitoramento de ativos em nuvem e serviços técnicos — conforme os limites máximos estabelecidos na Tabela do item 7.1 acima.
- 7.11.2. A obrigação financeira inicial da Administração vincular-se-á estritamente aos quantitativos mínimos indicados na referida tabela, a serem ativados mediante a emissão da primeira Ordem de Serviço (OS).
- 7.11.3. No entanto, resta assegurado à PRF a prerrogativa de solicitar a ativação das quantidades restantes de qualquer item, de forma fracionada ou integral, a qualquer tempo durante a vigência contratual, até o limite estabelecido pela quantidade máxima da referida tabela do TR, bastando para isso a emissão de novas Ordens de Serviço, de acordo com a necessidade institucional e a disponibilidade orçamentária.
- 7.11.4. Este modelo garante que o pagamento ocorra exclusivamente pelos serviços e licenças efetivamente disponibilizados e em uso, preservando o princípio da economicidade e evitando o desembolso por capacidades não utilizadas.

8. Levantamento de soluções

- 8.1 O principal objetivo deste Estudo Técnico Preliminar (ETP) é orientar a seleção da solução mais adequada, pautada em critérios de eficácia, efetividade, eficiência e viabilidade econômica, de modo a satisfazer plenamente às necessidades de negócio da PRF.
- 8.2 Portanto, para alcançar este objetivo, é crucial que a equipe de planejamento da contratação elabore critérios que viabilizem a comparação entre diversas soluções, tanto em termos de qualidade quanto de viabilidade econômica, ao mesmo tempo em que visa estabelecer uma base sólida para a tomada de decisões alinhadas aos objetivos estratégicos da instituição, de forma a proporcionar a escolha da melhor solução.
- 8.3 Foram identificadas 4 (quatro) possíveis soluções para a segurança da informação, conforme descrição da tabela a seguir:

Cenário	Descrição
1	Renovação do licenciamento das soluções de proteção de estações de trabalho, servidores (EPP, XDR, Deep Security) e proteção contra ameaças persistentes avançadas (DDI) já adquiridas.
2	Solução existente no Portal de Software Público Brasileiro.
3	Manter a solução atual sem garantia e sem suporte.
4	Renovação e ampliação do licenciamento, por demanda das soluções de proteção de estações de trabalho, servidores (EPP, XDR, Deep Security) e proteção contra ameaças persistentes avançadas (DDI) já adquiridas e inclusão da Solução para

9. Análise comparativa de soluções

9.1. A proteção física e lógica da informação deve ser provida por ferramentas especializadas, seguras, consolidadas e, acima de tudo, que preservem a confidencialidade, a integridade e a disponibilidade da informação.

9.2. A análise comparativa de soluções visa a elencar as alternativas de atendimento à demanda considerando, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

9.2.1. **Cenário 1** - Renovação do licenciamento das soluções de proteção de estações de trabalho, servidores (EPP, XDR, Deep Security) e proteção contra ameaças persistentes avançadas (DDI) já adquiridas. A primeira alternativa em avaliação envolve a renovação da solução de endpoints e servidores com a fabricante Trend Micro, visando preservar o investimento já realizado pela PRF por meio da renovação das licenças das ferramentas já adquiridas.

9.2.1.1. A PRF vem utilizando, com sucesso, por mais de 5 anos, as soluções da fabricante Trend Micro para proteção de estações de trabalho, servidores e proteção contra ameaças persistentes avançadas. As licenças foram adquiridas através dos Contratos Administrativos nº 1/2022 e nº 5/2021.

9.2.1.2. A solução adquirida à época foi atualizada para uma nova plataforma integrada de nome Trend Vision One, incluindo recursos como a capacidade de correlacionar eventos avançados e priorizar a resposta correspondente. Com esta solução, é possível visualizar o ciclo de vida de um ataque em toda a camada de rede, abrangendo dispositivos tanto gerenciados como não gerenciados.

9.2.1.3. Diante da necessidade de expansão do ambiente seguro da PRF, contextualizada em seções anteriores, apenas a renovação das licenças existentes não é desejável, tornando este cenário inviável, visto que haverá necessidade de proteção, também, para outros vetores de ataque que surgem a todo momento.

9.2.2. **Cenário 2** - Solução existente no portal de software público brasileiro.

9.2.2.1. Neste cenário foi analisada a possibilidade de usar as ferramentas disponíveis no Portal de Software Público Brasileiro para atender as necessidades específicas em questão.

9.2.2.2. Após uma pesquisa no Portal de Software Público (<https://www.gov.br/governodigital/pt-br/plataformas-e-servicos-digitais/softwarepublico/catalogo/catalogo>), verificou-se que não há programas que apresentem as características essenciais para a solução desejada. Portanto, a utilização de software público para fornecimento de licenças, suporte técnico, garantia e atualizações não é viável. Nesse contexto, é necessário contratar uma empresa especializada que possa atender às demandas com precisão. Por conta desta lacuna identificada, recomendamos que este cenário seja descartado, visto que não atende aos requisitos críticos estabelecidos pela PRF.

9.2.3. **Cenário 3** - Manter a solução atual sem garantia e sem suporte.

9.2.3.1. Esta solução compreende a não realização da renovação das licenças já utilizadas ou não realizar a aquisição de uma nova ferramenta de proteção de endpoints e servidores, mantendo somente as licenças que a PRF já possui, sem garantia e suporte do fabricante.

9.2.3.2. Assim, vale ressaltar que softwares desatualizados são uma relevante porta de entrada para cibercriminosos, uma vez que a falta de atualizações de segurança - criadas justamente como resposta a brechas de segurança - torna os sistemas altamente vulneráveis. A recente onda de ataques por

criptoransomware denominada "WannaCry", por exemplo, é uma ameaça que aproveita a falta de atualizações em sistemas operacionais Windows para invadir computadores. Este cenário não é viável para a PRF.

9.2.4. **Cenário 4** - Renovação e ampliação do licenciamento das soluções de proteção de estações de trabalho, servidores (EPP, XDR, Deep Security) e proteção contra ameaças persistentes avançadas (DDI) já adquiridas.

9.2.4.1. O cenário 4 envolve a renovação e ampliação do licenciamento das soluções de proteção já existentes para atender às necessidades da PRF. Nesse contexto, é crucial realizar uma análise detalhada das necessidades e requisitos de segurança da organização, garantindo que a solução seja capaz de satisfazer plenamente essas demandas. É fundamental que essa solução integre todas as "portas de entrada" de segurança, incluindo endpoints, proteção de aplicações, servidores físicos, virtuais e container, redes, bem como ofereça recursos avançados de Detecção e Resposta Estendida (XRD) por meio de uma única centralizadora de logs e detecções.

9.2.4.2. Para proporcionar uma avaliação mais precisa, considerando que o mercado de soluções corporativas de segurança de endpoints é diversificado e inclui várias opções, fizemos uma análise das principais soluções conhecidas no mercado, com base no review de Endpoint Protection Platform do Gartner (<https://www.gartner.com/reviews/market/endpoint-protection-platforms> acessado em maio/2025).

9.2.4.3. A partir desta consulta, foram selecionadas as seguintes soluções: Trellix Endpoint Security (ENS); Sophos Endpoint; Microsoft Defender for Endpoint; SentinelOne Singularity Platform; CrowdStrike Falcon; Trend Apex One; Elastic Security;

9.2.4.4. A análise de cada uma destas visa verificar se atendem plenamente as necessidades definidas nos requisitos deste estudo. A seguir, apresentam-se as principais características técnicas e recursos de cada solução:

1. **Trellix Endpoint Security (ENS):** EDR avançado com análise de comportamento; proteção baseada em machine learning; integração com soluções de segurança como SIEM e SOAR; controle de dispositivos USB e whitelisting de aplicações; suporte a sandboxing e firewall integrado; gestão centralizada via console; foco em resposta rápida e automação de remediações.
2. **Sophos Intercept X Endpoint:** Combina EDR com inteligência artificial para bloqueio de ameaças avançadas; exploit prevention e proteção contra ransomware com rollback de ações; sandboxing para análise de arquivos suspeitos; integração com a plataforma de gerenciamento central Sophos Central; controle de aplicativos, firewall integrado e DLP; oferece proteção para dispositivos móveis.
3. **Microsoft Defender for Endpoint:** EDR e XDR integrados com o ecossistema Microsoft; proteção contra exploits e ransomware; gestão centralizada através do Microsoft 365 Defender; Machine learning e análise de comportamento para detecção proativa; proteção multinuvem e integração com SIEM e SOAR; suporte para ambientes híbridos (on-premises e nuvem).
4. **SentinelOne Singularity Platform:** EDR e XDR com foco em automação total de respostas a ameaças; proteção baseada em IA e análise comportamental; suporte para rollback de ransomware e análise forense; integração com SIEM e ferramentas de segurança para respostas coordenadas; proteção para workloads em nuvem, contêineres e ambientes virtualizados.
5. **CrowdStrike Falcon:** EDR em tempo real com análise baseada em inteligência artificial; detecção baseada em comportamento e hunting de ameaças; proteção multinuvem e integração com outras ferramentas de segurança; gestão centralizada via Falcon Platform; análises forenses e automação de resposta a incidentes; suporte para proteção de endpoints, servidores e dispositivos móveis.
6. **Trend Apex One:** EDR com foco em análise de comportamento e machine learning; proteção contra ransomware e vulnerabilidades; gestão de vulnerabilidades e proteção para workloads em nuvem; firewall integrado, sandboxing e suporte para ambientes multinuvem; proteção de e-mails e colaboração, além de controle de dispositivos; suporte a ambientes virtualizados e contêineres.

7. **Elastic Security:** solução de segurança unificada que combina SIEM (Gerenciamento de Informações e Eventos de Segurança) e XDR (Detecção e Resposta Estendidas), incluindo EDR (Detecção e Resposta de Endpoint) através do Elastic Defend. Suas principais funcionalidades incluem a ingestão e análise em larga escala de dados de segurança de diversas fontes, detecção de ameaças avançadas usando machine learning e análise comportamental, prevenção contra malware e ransomware nos endpoints, e ferramentas robustas para investigações forenses e threat hunting. É gerenciado centralmente via Kibana, permitindo respostas rápidas e orquestração de ações de remediação em ambientes on-premises, multinuvem e de contêineres.

9.3. Foi realizada uma análise consolidada das soluções e das funcionalidades, com o objetivo de verificar o grau de atendimento às necessidades de segurança cibernética da PRF.

9.3.1. Neste cenário foram avaliados como critérios de seleção a presença das funcionalidades abaixo listadas, que são essenciais para o fortalecimento do ambiente de cibersegurança, bem como o atendimento aos controles do Programa de Privacidade e Segurança da Informação - PPSI do Governo Federal:

9.3.1.1. **Proteção antivírus/anti-malware:** detecta, bloqueia e remove vírus, malwares e outras formas de software malicioso que possam infectar o sistema. Atua com assinatura de ameaças conhecidas e, em alguns casos, com análise heurística para detectar comportamentos maliciosos. Firewall integrado: controla o tráfego de rede que entra e sai dos endpoints, bloqueando acessos não autorizados e prevenindo ataques baseados em rede, como tentativas de intrusão ou exploração de vulnerabilidades.

9.3.1.2. **EDR (Detecção e Resposta a Ameaças):** fornece monitoramento contínuo e resposta automatizada a ameaças avançadas nos endpoints, identificando comportamentos suspeitos e permitindo investigações detalhadas e remediação rápida.

9.3.1.3. **XDR (Extended Detection and Response):** expande as capacidades do EDR para coletar e correlacionar dados de múltiplas fontes (como rede, nuvem, e-mail) e fornecer uma visão unificada das ameaças em várias superfícies de ataque.

9.3.1.4. **Machine Learning para detecção de ameaças:** utiliza algoritmos de aprendizado de máquina para identificar padrões e comportamentos anômalos, permitindo a detecção de novas ameaças que ainda não foram catalogadas (zero-day threats).

9.3.1.5. **Proteção contra exploits:** previne o uso de vulnerabilidades conhecidas em software e sistemas para comprometer endpoints, bloqueando ataques que exploram falhas de segurança, como buffer overflows ou execução de código remoto.

9.3.1.6. **Proteção ransomware:** detecta e bloqueia ataques de ransomware antes que eles possam criptografar arquivos, utilizando técnicas de monitoramento de comportamento e bloqueio de atividades suspeitas que indicam um ataque.

9.3.1.7. **Gerenciamento centralizado (Console):** fornece uma plataforma unificada para gerenciar a segurança de todos os dispositivos protegidos. Permite que administradores apliquem políticas, monitorem ameaças e tomem ações corretivas de forma centralizada.

9.3.1.8. **Prevenção de Perda de Dados (DLP):** monitora e controla o fluxo de dados sensíveis para prevenir que informações confidenciais sejam transmitidas ou acessadas indevidamente, tanto dentro como fora da organização.

9.3.1.9. **Controle de dispositivos:** monitora e gerencia o uso de dispositivos periféricos, como USBs e discos externos, para evitar que dispositivos não autorizados sejam usados para introduzir malwares ou extrair dados.

9.3.1.10. **Whitelisting de aplicações:** permitir que apenas aplicativos pré-aprovados (em uma lista branca) sejam executados no endpoint, prevenindo a execução de software malicioso ou não autorizado.

9.3.1.11. **Proteção para dispositivos móveis:** fornece segurança para smartphones e tablets, incluindo proteção contra malwares, controle de aplicativos, e gestão de dispositivos móveis (MDM), para proteger dados e acessos corporativos.

9.3.1.12. **Proteção em ambientes multinuvem:** oferece segurança para workloads e dados que estão em execução em várias plataformas de nuvem (como AWS, Azure e Google Cloud), monitorando e protegendo contra ameaças específicas da nuvem.

9.3.1.13. **Segurança para e-mails e colaboração:** protege sistemas de e-mail e plataformas de colaboração (como Microsoft 365, Zimbra e Google Workspace) contra phishing, malwares e roubo de credenciais, prevenindo ataques por anexos maliciosos ou links de phishing.

9.3.1.14. **Análises forenses:** fornece ferramentas para investigar a origem e a natureza de uma ameaça ou ataque, permitindo que os analistas de segurança identifiquem a causa raiz e ajustem as defesas.

9.3.1.15. **Rollback de ações maliciosas:** reverte as mudanças feitas por ataques, como a remoção de malwares e a recuperação de arquivos criptografados por ransomware, restaurando o sistema ao seu estado anterior à infecção.

9.3.1.16. **Proteção para ambientes virtualizados:** protege máquinas virtuais e infraestruturas virtualizadas (como VMware, Hyper-V), detectando e bloqueando ameaças específicas para esses ambientes, incluindo a proteção de hypervisors e VMs.

9.3.1.17. **Suporte a contêineres e workloads em nuvem:** protege contêineres (como Docker e Kubernetes) e workloads em execução na nuvem, monitorando vulnerabilidades e comportamentos anômalos nesses ambientes.

9.3.1.18. **Deteção baseada em comportamento (Behavioral Analysis):** monitora o comportamento de processos e aplicativos em tempo real para identificar atividades suspeitas que indicam possíveis ameaças, mesmo que essas ameaças sejam desconhecidas.

9.3.1.19. **Sandboxing (análise de arquivos suspeitos):** executa arquivos suspeitos em um ambiente isolado (sandbox) para verificar seu comportamento e determinar se são maliciosos, sem risco de infectar o sistema real.

9.3.1.20. **Capacidades de Threat Hunting:** fornece ferramentas para analistas de segurança buscarem ativamente por ameaças que podem estar ocultas ou que ainda não foram detectadas automaticamente, permitindo investigações mais detalhadas e proativas.

MAPA COMPARATIVO DE FUNCIONALIDADES							
Funcionalidade	Trellix Endpoint Security	Sophos Endpoint;	Microsoft Defender for Endpoint;	SentinelOne Singularity Platform	CrowdStrike Falcon;	Trend Apex One	Elastic Security
Proteção antivírus/anti-malware	Sim	Sim	Sim	Sim	Sim	Sim	Sim
EDR (Deteção e Resposta a Ameaças)	Sim	Sim	Sim	Sim	Sim	Sim	Sim
XDR (Extended							

Detection and Response)	Não	Não	Sim	Sim	Sim	Sim	Sim
Machine Learning para detecção de ameaças	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Proteção contra exploits	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Proteção ransomware	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Gerenciamento centralizado (Console)	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Prevenção de Perda de Dados (DLP)	Não	Sim	Não	Não	Não	Sim	Não
Controle de dispositivos	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Whitelisting de aplicações	Sim	Sim	Não	Sim	Sim	Sim	Sim
Proteção para dispositivos móveis	Sim	Sim	Sim	Sim	Sim	Sim	Não
Proteção em ambientes multinuvem	Não	Sim	Sim	Sim	Sim	Sim	Sim
Segurança para e-mails e colaboração	Não	Sim	Sim	Não	Não	Sim	Não
Análises forenses	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Rollback de ações maliciosas	Não	Sim	Sim	Sim	Sim	Sim	Não
Proteção para ambientes virtualizados	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Suporte a contêineres e workloads em nuvem	Não	Sim	Sim	Sim	Sim	Sim	Sim
Detecção baseada em comportamento (Behavioral Analysis)	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Sandboxing							

(análise de arquivos suspeitos)	Não	Sim	Sim	Sim	Sim	Sim	Não
Capacidades de Threat Hunting	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Resultado da comparação	Não atende na Totalidade	Não atende na Totalidade	Não atende na Totalidade	Não atende na Totalidade	Não atende na Totalidade	Atende	Não atende na Totalidade

* Os itens que são atendidos apenas parcialmente foram elencados na tabela como "Não", por não atenderem as funcionalidades em sua totalidade.

9.4. Conforme a análise demonstrada, unicamente a plataforma Trend Micro Apex One satisfaz integralmente as exigências estabelecidas nos critérios avaliados.

9.5. A Trend Micro Apex One provê um elevado nível de proteção contra ameaças sofisticadas, com ênfase em ameaças de dia zero (zero-day threats), além de robusta cobertura para infraestruturas virtualizadas e contêineres, e eficiente integração com sua plataforma XDR, Vision One. Revela-se particularmente vantajosa para entidades que empregam tecnologias de nuvem e contêineres como componentes cruciais de suas atividades.

9.6. Após minuciosa avaliação comparativa entre as plataformas, a Polícia Rodoviária Federal (PRF) decidiu pela manutenção e ampliação da solução Trend Micro. Esta deliberação foi fundamentada em um conjunto de fatores alinhados às necessidades operacionais e estratégicas do Departamento, ponderando elementos como a estabilidade do ambiente tecnológico, a curva de aprendizado da equipe, o cronograma de migração e a confiança no atual provedor de serviços.

9.7. A seguir, detalhamos a justificativa, explicitando as razões de ordem técnica e operacional que consolidam a Trend Micro Apex One como a plataforma mais adequada para a PRF.

9.7.1. Estabilidade e Confiabilidade do Ambiente Existente: A PRF já emprega a solução Trend Micro em uma parcela significativa de sua infraestrutura tecnológica. A confiabilidade demonstrada pela plataforma ao longo de cerca de 5 anos de utilização, sem paralisações operacionais significativas ou incidentes de segurança de maior impacto, consolida a confiança na preservação deste ambiente. Ao optar pela continuidade com a Trend Micro, o Departamento mitiga os riscos de descontinuidade das operações críticas, que poderiam advir de desafios de integração ou de um extenso processo de migração, salvaguardando o legado de performance estável.

9.7.1.1. A implementação de uma nova plataforma de segurança, demandaria um período de transição e potencial vulnerabilidade sistêmica, o que é inadmissível, dada a natureza crítica e ininterrupta das operações da PRF, essenciais para a segurança viária nacional. Tal mudança poderia não apenas fragilizar o ambiente de segurança a curto prazo, mas também impor uma carga de trabalho adicional às equipes de tecnologia e segurança durante a adaptação a uma nova ferramenta. Adicionalmente, é imperativo considerar que a manutenção e expansão da solução Trend Micro na PRF oferecem vantagens técnicas, operacionais e de segurança vitais para a proteção da instituição.

9.7.1.2. A Trend Micro dispõe de tecnologias avançadas de cibersegurança que protegem contra ameaças conhecidas e emergentes. Recentemente, diversas entidades da Administração Pública Federal (APF) enfrentaram um volume crescente de incidentes cibernéticos, como invasões de sistemas, ataques de ransomware e exfiltração de dados. Exemplos notórios incluem os ataques ao Ministério da Gestão e Inovação; à Casa da Moeda Brasileira, ao Conselho de Controle de Atividades Financeiras, e a múltiplos Ministérios (Desenvolvimento, Fazenda, Igualdade Racial, Microempresa, Mulheres, Planejamento, Previdência Social, Povos Indígenas); à Agência Nacional de Águas; e ao Superior Tribunal de Justiça. Tais eventos sublinham a imperatividade de uma solução de segurança resiliente e confiável para a salvaguarda do ambiente institucional da PRF.

9.7.2. Facilidade de Expansão e Reduzido Tempo de Adaptação: A continuidade com a Trend Micro assegura um menor tempo de capacitação técnica, uma vez que o corpo técnico da PRF já possui domínio sobre a interface, as funcionalidades e as melhores práticas da solução. Mantendo essa familiaridade, a PRF otimiza o emprego de tempo e recursos, pois o conhecimento prévio da plataforma do fabricante torna a assimilação de novas funcionalidades mais eficaz e ágil. Em contraste, a adoção da Symantec exigiria um investimento considerável em treinamento das equipes de TI e segurança, além de um esforço suplementar para configurar e integrar a nova solução aos sistemas legados e operacionais. O período de adaptação e o ajuste de políticas de segurança em uma nova plataforma poderiam comprometer a celeridade na resposta a incidentes e afetar o cumprimento das rotinas operacionais durante a transição.

9.7.3. Tempo e Complexidade de Migração: O processo de transição para uma nova plataforma de segurança acarreta desafios substanciais, especialmente quando a infraestrutura tecnológica já se encontra consolidada com uma plataforma específica. A migração integral dos ativos instalados para a solução Symantec demandaria um planejamento detalhado e execução meticulosa para prevenir falhas de segurança ou perda de informações críticas, considerando que a implantação envolveria as unidades centrais de todos os estados brasileiro e da UNIPRF. Por outro lado, a permanência com a plataforma Trend Micro suprime a necessidade dessa transição laboriosa, permitindo que a PRF continue a usufruir das funcionalidades já estabelecidas, enquanto expande a cobertura para novas áreas e serviços de maneira integrada. Isso garante uma continuidade operacional fluida, isenta de interrupções ou riscos adicionais.

9.7.4. Recursos Funcionais e Alinhamento às Necessidades da PRF: A escolha pela Trend Micro não se baseou apenas na confiança preexistente, mas também em sua capacidade de atender a todas as áreas críticas de segurança da PRF, incluindo:

- **Proteção de estações de trabalho, servidores e sistemas operacionais:** A Apex One oferece defesa robusta contra ameaças conhecidas e emergentes, com capacidade de detecção de ataques avançados em todos os endpoints e servidores que sustentam as operações da PRF.
- **Segurança para ambientes de desenvolvimento, virtualização e dados sensíveis:** Suporte avançado para a segurança de infraestruturas de desenvolvimento, ambientes virtualizados e repositórios de dados críticos, cruciais em arquiteturas modernas, assegurando que a PRF possa operar com segurança mesmo em cenários de alta complexidade tecnológica.
- **Defesa para dispositivos móveis operacionais e mitigação de ameaças via e-mail:** A integração de proteção para dispositivos móveis utilizados em campo e funcionalidades antispam robustas fortalecem a defesa contra ataques direcionados por e-mail e através de comunicações móveis, vetores comuns de ameaças.
- **Gestão proativa da superfície de exposição a ataques cibernéticos:** A Trend Micro provê uma visão consolidada da superfície de ataque, capacitando a PRF a identificar e mitigar vulnerabilidades antes que se convertam em ameaças ativas contra a instituição.
- **Considerando a utilização estratégica pela Polícia Rodoviária Federal dos ambientes de nuvem Azure, AWS e GCP,** que expandem significativamente sua superfície de ataque digital, a solução Trend Vision One - Attack Surface Risk Management for Cloud apresenta-se como um componente essencial para a segurança proativa e integrada das operações da PRF. Esta ferramenta é projetada especificamente para prover visibilidade contínua e abrangente sobre os ativos, configurações e potenciais vulnerabilidades nesses múltiplos provedores de nuvem, identificando automaticamente recursos expostos, configurações incorretas e riscos de conformidade. Ao fornecer uma análise contextualizada e priorizada dos riscos cibernéticos específicos do ecossistema de nuvem da PRF, o Attack Surface Risk Management for Cloud alinha-se diretamente com a necessidade institucional de uma "Gestão proativa da superfície de exposição a ataques cibernéticos", capacitando o Departamento a identificar, avaliar e mitigar vulnerabilidades e ameaças em seus serviços e dados críticos hospedados na nuvem antes que possam ser explorados, complementando assim a proteção já existente em outras camadas da infraestrutura tecnológica.

9.8. Embora outras plataformas também disponibilizem um conjunto abrangente de funcionalidades, a Trend Micro se sobressai por oferecer uma solução já consolidada no ambiente da PRF, com recursos avançados de inteligência

contra ameaças e integração transparente em diversos contextos tecnológicos. A adaptabilidade da Trend Micro à infraestrutura existente da PRF e sua capacidade de expansão para novas áreas de segurança tornam esta solução a mais congruente com as necessidades do Departamento.

9.9 Confiança no Fornecedor e Relacionamento com a Trend Micro: A parceria tecnológica consolidada entre a PRF e a Trend Micro representa um fator preponderante nesta decisão. A credibilidade do suporte especializado, do atendimento às demandas e da agilidade na resolução de problemas emergentes é fundamental para assegurar a solidez e resiliência das operações de segurança. Adicionalmente, a Trend Micro tem demonstrado uma capacidade contínua de inovação, mantendo sua plataforma atualizada e alinhada com as novas ameaças do panorama cibernético global. Em contrapartida, a transição para um novo fornecedor, como a Symantec Endpoint Security Complete, implicaria riscos substanciais, incluindo a necessidade de construir um novo relacionamento institucional. Esse processo de adaptação envolveria uma fase de adaptação e possíveis incertezas, com potenciais desafios relacionados à tempestividade do suporte e à familiaridade com o ambiente operacional da PRF. Manter o relacionamento com a Trend Micro evita tal risco e preserva a continuidade das operações, sem interrupções que poderiam comprometer a segurança da instituição em um momento crítico.

9.10. Custo Total de Propriedade (TCO) e Otimização de Recursos: Outro elemento decisivo é o Custo Total de Propriedade (TCO). A manutenção da plataforma Trend Micro representa a maximização dos investimentos pretéritos, garantindo que a PRF continue a usufruir de economias de escala e suporte técnico eficiente, sem a necessidade de reestruturar seus processos de segurança. Manter e expandir a solução atual pode proporcionar economias de escala significativas, visto que o incremento no licenciamento tende a reduzir o custo unitário de proteção. Ademais, a uniformização da solução de segurança cibernética simplifica o gerenciamento centralizado, otimizando a operação e reduzindo os custos indiretos associados à instalação, capacitação, manutenção e suporte técnico. É possível inferir que a economicidade se manifesta claramente, pois, ao permitir a contratação fragmentada de diferentes soluções para atender aos diversos itens de um eventual certame, a instituição seria compelida a contratar, para cada solução adjudicada, serviços distintos de instalação, treinamento de equipe, suporte técnico e integração entre as diversas ferramentas. Isso resultaria em uma multiplicidade de contratos a serem gerenciados e fiscalizados, sobrecarregando a equipe com demandas adicionais de tempo, administração e resolução de conflitos. Propostas de alteração por parte de fornecedores que desconhecem as particularidades operacionais e os imperativos de segurança da PRF podem subestimar os desafios de interoperabilidade, as potenciais brechas de segurança durante a transição e o risco de ciclos licitatórios adicionais para assegurar a continuidade da proteção institucional.

9.11. Abaixo segue uma análise de requisitos relevantes da solução nº 04:

Requisito	Cenário	SIM	NÃO	NÃO SE APLICA
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	1	X		
	2	X		
	3		X	
	4		X	
A Solução está disponível no Portal do Software Público Brasileiro?	1		X	
	2		X	
	3		X	
	4		X	
A Solução é um software livre ou software público?	1		X	
	2		X	
	3		X	
	4		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	1	X		
	2	X		
	3		X	
	4	X		

A Solução é aderente às regulamentações da ICPBrasil? (quando houver necessidade de certificação digital)	1			X
	2			X
	3			X
	4			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	1			X
	2			X
	3			X
	4			X

9.12. Definição da Solução Viável para a PRF

Reconhece-se que um dos escopos dos certames públicos é garantir a equidade de tratamento a todos os participantes, consolidando, assim, o princípio constitucional da isonomia. Contudo, para a concretização desse escopo, é imperativo observar que o propósito fundamental do processo licitatório é a seleção da proposta que melhor atenda ao interesse da Administração Pública. Nesse sentido, é pertinente o entendimento do Superior Tribunal de Justiça:

- “ADMINISTRATIVO. PROCEDIMENTO LICITATÓRIO. AUTORIA. EMPRESA. LEGALIDADE. Quando, em procedimento licitatório, exige-se comprovação, em nome da empresa, não está sendo violado o art. 30 §1º, II, caput, da Lei 8.666/1993. É de vital importância, no trato da coisa pública, a permanente perseguição ao binômio qualidade e eficiência, objetivando não só garantir a segurança jurídica do contrato, mas também a consideração de certos fatores que integram a finalidade das licitações, máxime em se ao administrador a elaboração de dispositivos, sempre em atenção à pedra de toque do ato administrativo – a lei – mas com dispositivos que busquem resguardar a Administração de aventureiros ou de licitantes de competência estrutural, administrativa e organizacional duvidosa.” Recurso provido. (Resp. nº 44.750-SP, rel. Ministro Francisco Falcão, 1ª T., unânime, DJ de 25.9.00)
- A Lei nº 14.133/2021 não apenas mantém, mas reforça a necessidade de a Administração Pública buscar a qualidade, a eficiência e a segurança jurídica em seus contratos. Os mecanismos de planejamento, análise de riscos, qualificação dos licitantes e os critérios de julgamento são todos voltados para garantir que a proposta selecionada seja verdadeiramente a mais vantajosa, protegendo o interesse público contra licitantes sem a devida competência estrutural, administrativa ou organizacional. Assim, o entendimento do STJ sobre a importância de resguardar a Administração de "aventureiros" permanece plenamente aplicável e, de certa forma, instrumentalizado de maneira ainda mais robusta pela nova legislação.

9.13. Dessa forma, o intuito da Administração não é simplesmente recepcionar, nos processos licitatórios, qualquer tipo de solução singular ou destoante do objeto almejado, mas sim assegurar uma disputa abrangente focada no suprimento efetivo de suas demandas.

9.14. Considerando o exposto, o único panorama factível para a Polícia Rodoviária Federal (PRF) consiste na contratação de uma plataforma integrada para a proteção de seus ativos digitais, abrangendo estações de trabalho, servidores, dispositivos móveis, contêineres, ambientes de colaboração, bem como o gerenciamento de riscos e da superfície de ataque. Nesta avaliação, foram confrontadas oito soluções de segurança de distintos fabricantes. Com base na ponderação de elementos cruciais, como estabilidade operacional, cronograma de migração, confiabilidade do provedor atual e a capacidade de suprir as exigências de segurança da PRF, as soluções da Trend Micro emergem como a opção mais congruente. Sua manutenção e expansão asseguram uma abordagem de segurança robusta, confiável e eficaz, permitindo à PRF proteger seu ambiente tecnológico em constante evolução e criticidade.

9.15. Nesse sentido, é crucial reiterar que a seleção da plataforma de segurança deve ser orientada pelas demandas específicas da PRF, pelas características de seu ambiente de TI, pelos princípios de economicidade e pelas prioridades de segurança da Instituição. Embora as alternativas tecnológicas avaliadas neste estudo apresentem consistência em termos de funcionalidades de segurança, a Trend Micro distingue-se por oferecer recursos essenciais ao pleno atendimento das necessidades da Polícia Rodoviária Federal.

9.16. A decisão pela manutenção da marca fundamenta-se nos princípios da uniformização da infraestrutura tecnológica, da continuidade da solução e da unificação da ferramenta de gerenciamento. Dessa maneira, a equipe

de tecnologia da informação da PRF, responsável pela segurança cibernética, pode implementar políticas de segurança coesas e uniformes, eliminando potenciais prejuízos decorrentes de eventuais incompatibilidades sistêmicas. O princípio da padronização e da continuidade da solução coaduna-se com os preceitos da legalidade, finalidade, economicidade, interesse público e vantajosidade para a Administração Pública Federal (APF), sem detrimento aos demais princípios norteadores das aquisições de bens, produtos e serviços pela APF.

9.17. Por imperativos estratégicos e operacionais, é fundamental empregar produtos que possuam configuração, manutenção e operacionalidade idênticas ou análogas àquelas atualmente implementadas na PRF. Tal abordagem torna o processo de implantação, operação e transferência de conhecimento simplificado, mais ágil e com reduzidos riscos e impactos adversos às atividades finalísticas da Instituição, que são indelegáveis e de natureza crítica para a segurança pública. O corpo técnico da PRF acumulou experiência prática substancial na gestão de incidentes e na resolução de problemas durante o período de utilização da solução vigente. Dispor dessa expertise consolidada assegura condições otimizadas para a identificação e solução de ocorrências, bem como para o controle e fiscalização dos serviços de segurança contratados, permitindo sua resolução eficaz e o acompanhamento rigoroso dos serviços. A continuidade da solução demonstra-se vantajosa por ter comprovado, ao longo de sua utilização, sua capacidade de atender aos requisitos de segurança da PRF, mostrando-se eficaz e efetiva tanto na proteção preventiva de estações de trabalho e servidores quanto na correção, solução e tempo de resposta em eventuais incidentes que poderiam comprometer as operações policiais.

9.18. Ao se permitir uma multiplicidade excessiva de fornecedores, além da perda de homogeneidade e padronização da solução de segurança, haveria um risco manifesto de desencontro no provimento dos componentes da plataforma, podendo gerar vulnerabilidades e dificultar a gestão integrada da segurança. Dessa forma, a aceitação da adjudicação por item desvirtua a concepção de uma Solução de Tecnologia da Informação coesa, pois resultaria na perda irreparável da capacidade de integração dos serviços e do potencial de compartilhamento de recursos e inteligência de ameaças – condições estas que não podem ser garantidas apenas por meio de especificações técnicas isoladas. Portanto, a estruturação proposta para a contratação agrupa, de maneira lícita, segura, técnica e economicamente viável, serviços de mesma natureza que mantêm correlação intrínseca, seja por similaridade técnica ou tecnológica, bem como por aplicabilidade e configuração do modelo de contratação, sem impor qualquer restrição à ampla competitividade.

9.19. A PRF ponderou igualmente o investimento já efetuado e o benefício da curva de aprendizado consolidada (onboarding) da equipe técnica, visando reduzir o tempo de adaptação e otimizar o período de atualização e emprego das ferramentas de segurança. Os benefícios desta estratégia são reforçados por aspectos técnicos que corroboram esta decisão, tais como:

9.19.1. **Gerenciamento Centralizado das Tecnologias:** A centralização na administração das tecnologias de segurança permite uma gestão mais eficiente e coesa de todos os recursos, facilitando a aplicação de políticas, o monitoramento e a manutenção em toda a infraestrutura de TI da PRF.

9.19.2. **Integração Ativa entre as Soluções de Segurança:** A interconexão entre as diversas camadas da solução de segurança promove uma abordagem holística na proteção do ambiente tecnológico, assegurando que cada componente opere em sinergia para robustecer a segurança global e prover uma defesa sólida contra ameaças cibernéticas direcionadas às operações policiais.

9.19.3. **Visão Unificada por Meio de Console Única:** A disponibilidade de um painel de controle único oferece uma perspectiva centralizada e integrada de todas as operações de segurança, simplificando a administração, o monitoramento e a análise de eventos em tempo real. Esta abordagem unificada permite uma resposta mais célere e efetiva a incidentes, garantindo uma postura defensiva mais proativa e resiliente para a Polícia Rodoviária Federal.

10. Registro de soluções consideradas inviáveis

10.1. Conforme estipulado no § 1º do art. 11 da Instrução Normativa SGD/ME n.º 94/2022, todas as soluções identificadas como inviáveis devem ser devidamente registradas no Estudo Técnico Preliminar da Contratação, acompanhadas de uma breve descrição e justificativa. Esse registro dispensa a necessidade de elaborar os cálculos de custo total de propriedade.

10.2. Com base nas análises detalhadas apresentadas neste documento, as seguintes soluções foram consideradas inviáveis:

10.2.1. Renovação do licenciamento das soluções de proteção de estações de trabalho, servidores (EPP, XDR, Deep Security) e proteção contra ameaças persistentes avançadas (DDI) já adquiridas.: diante da necessidade de expansão do ambiente seguro da PRF para cobertura de outros vetores de ataque, apenas a renovação das licenças existentes não é desejável para a PRF, tornando este cenário inviável.

10.2.2. Solução disponível no Portal de Software Público Brasileiro: a pesquisa realizada no Portal de Software Público brasileiro não revelou nenhuma solução que atenda às necessidades específicas, tornando essa opção inviável.

10.2.3. Manter a solução atual sem garantia e sem suporte: torna-se um alto risco manter a solução atual sem garantia, atualizações e suporte, visto que os ataques cibernéticos estão cada vez mais sofisticados e impactantes.

10.3. Registre-se que também foram realizadas pesquisas, tanto em Intenções de Registro de Preços abertas no período de elaboração deste Estudo Técnico, bem como em possíveis registros de preços já concluídos, para verificar a existência de alguma contratação que se amoldasse à demanda da PRF, porém, não foram encontradas alternativas que se alinhassem quantitativamente e/ou qualitativamente à nossa necessidade.

11. Análise comparativa de custos (TCO)

11.1. Considerando que após a análise realizada, que se encontra detalhada no tópico 9 do presente estudo técnico, restou-se identificada apenas uma solução técnica e funcionalmente viável, a análise comparativa de custos, que deve, preferencialmente, ser realizada apenas entre as soluções consideradas viáveis, restou prejudicada, justamente por não ter sido identificada pelo menos uma segunda solução viável para ser confrontada com aquela apontada como mais adequada.

11.2. Porém, como dito alhures, A manutenção da plataforma Trend Micro representa um melhor aproveitamento, com extensão dos investimentos já realizados na solução, garantindo que a PRF continue a usufruir de economias de escala e suporte técnico eficiente, sem a necessidade de reestruturar seus processos de segurança.

11.3. Manter e expandir a solução atual pode proporcionar economias de escala significativas, visto que o incremento no licenciamento tende a reduzir o custo unitário de proteção. Ademais, a uniformização da solução de segurança cibernética simplifica o gerenciamento centralizado, otimizando a operação e reduzindo os custos indiretos associados à instalação, capacitação, manutenção e suporte técnico.

12. Descrição da solução de TIC a ser contratada

12.1. A solução que se deseja adquirir será composta pelas seguintes soluções/funcionalidades /características:

12.1.1. Solução de EPP e XDR (Plataforma de proteção de endpoint com detecção e resposta a ameaças): solução implantada em dispositivos endpoint para evitar ataques de malware baseados em arquivos, detectar atividades maliciosas e fornecer os recursos de investigação e correção necessários para responder a incidentes e alertas de segurança dinâmicos, incluindo software, gerenciamento centralizado, licenciamento, suporte técnico e garantia pelo período contratual; Monitoramento e resposta contínuos a ameaças avançadas de segurança cibernética, incluindo software, gerenciamento centralizado, licenciamento, suporte técnico e garantia pelo período contratual.

12.1.2. Solução de contra APT (Proteção Contra Ameaças Persistentes Avançadas): solução de monitoramento contínuo que oferece visibilidade em tempo real, contra ameaças avançadas, como exploits de zero-day e malwares personalizados, que se caracterizam por serem desconhecidas, direcionadas e evasivas, tornando

ineficientes as ferramentas de antivírus baseadas apenas em assinaturas para detecção de conteúdo malicioso, incluindo software, gerenciamento centralizado, licenciamento, suporte técnico e garantia pelo período contratual;

12.1.3. Solução para proteção de aplicações, servidores físicos, virtuais e container, gerenciamento centralizado, licenciamento, suporte técnico e garantia pelo período contratual;

12.1.4. Solução para visibilidade contínua, avaliação de riscos e priorização de ações para a superfície de ataque em ambientes de nuvem, gerenciamento centralizado, licenciamento, suporte técnico e garantia pelo período contratual;

12.2. As soluções deverão ser todas de um único fabricante;

12.3. As soluções poderão ser ofertadas no modelo SaaS com disponibilidade mínima de 99,8% para todas as funcionalidades, em cada mês civil;

12.4. A console de gerenciamento deve ser acessível em qualquer ponto da rede da contratante sem a necessidade de uma conexão VPN;

12.5. A console de gerenciamento deverá permanecer acessível por pelo menos 90 (noventa) dias após o término da vigência contratual.

12.6. Os softwares que compõem a solução (ou appliances, se for o caso) devem ser oferecidos na última versão disponibilizada pelo fabricante.

12.7. Na data da proposta, nenhum dos softwares ou appliances ofertados poderão estar listados pelo fabricante com data definida para fim de suporte ("end of support") ou fim de vendas ("end of sale").

12.8. Deverá ser apresentado diagrama detalhado com as soluções ofertadas, abrangendo todo o conjunto de softwares, aplicação e gerenciamento unificado;

12.9. A licitante deverá comprovar sua capacidade técnico-operacional por meio de atestado(s) de capacidade técnica que demonstre(m) a execução satisfatória de serviços ou soluções similares, compatíveis em complexidade tecnológica e operacional, equivalente ou superior, relacionados às parcelas de maior relevância do objeto licitado;

12.10. Serviço de instalação, transição e configuração; suporte e atualizações.

12.10.1. Consideram-se Serviços Técnicos Especializados as atividades de alta complexidade técnica que extrapolam a manutenção rotineira e o suporte de níveis 1 e 2, compreendendo exclusivamente:

a) Implantação e Configuração de APT/DDI: Instalação física ou lógica (virtual appliance), configuração de sensores de tráfego de rede e ajuste fino de regras de detecção nas unidades regionais e Sede.

b) Suporte Técnico de Nível 3 (Fabricante): Atendimento especializado prestado diretamente pelo desenvolvedor da solução ou por parceiro certificado de nível superior, para resolução de incidentes críticos, vulnerabilidades de "dia zero" ou instabilidades sistêmicas complexas.

c) Apoio à Resposta a Incidentes e Forense: Atividades de extração de evidências, análise de vetores de ataque e execução de planos de remediação em caso de comprometimento da infraestrutura.

d) Integração de Nuvem e APIs: Configuração de conectores para ambientes multinuvem (AWS, Azure, GCP, Huawei, IBM, Oracle) e integração via REST API com ferramentas de SIEM de terceiros.

12.11. As Especificações Técnicas da Solução detalhadas constam no Anexo I-B do Termo de Referência.

13. Estimativa de custo total da contratação

Valor (R\$): 14.156.385,00

13.1. Adotou-se como estimativa inicial do custo total da contratação o valor de **quatorze milhões, cento e cinquenta e seis mil, trezentos e oitenta e cinco reais ao ano**; valor este oriundo da média de propostas formais apresentados por empresas e por pregões anteriores com produtos/serviços similares, coletados no Painel de preços.

13.2. Sublinhe-se que tal estimativa poderá variar para mais ou para menos, especialmente após a realização de pesquisa de mercado em etapas posteriores do processo de contratação do serviço de TIC.

ESTIMATIVA - MEMÓRIA DE CÁLCULO (quantidade Mínima e Máxima) ao ano								
Item	Descrição do Objeto	Quant.	Unid.	Empresa Alltech	Pregão nº 90009 /24 CNPQ	Pregão nº 90958 /24 Dataprev	Pregão nº 90053 /24 Univ. Lavras	Média do valor unitário
1	TrendMicro Vision one Essential (XDR nativo)	11.182	Host	R\$ 163,00	R\$ 351,82	R\$ 220,20	R\$ 175,90	R\$: 227,72
2	Créditos TrendMicro Vision One (Sandbox)	225.000	Créditos	R\$ 6,00				R\$: 6,00
3	TrendMicro DDI COM XDR	8	Gb/s	R\$ 300.000,00				R\$: 300.000,00
4	TrendMicro Vision One Pro (XDR nativo)	300	Servers	R\$ 2.000,00				R\$: 2.000,00
5	Trend Vision One - Attack Surface Risk Management for Cloud	3	Ativos	R\$ 90.000,00				R\$: 90.000,00
6	Serviço de Suporte	12	Meses	R\$ 7.000,00	R\$ 9.450,00		R\$ 7.500,00	R\$: 7.983,33
7	Serviço de Implantação DDI	0	Serviço	R\$ 25.000,00				R\$ 25.000,00
CÁLCULOS COM QUANTITATIVOS MÍNIMOS								
Item nº 01				11.182 * R\$: 227,72		R\$: 2.546.365,04		
Item nº 02				225.000* R\$: 6,00		R\$: 1.350.000,00		
Item nº 03				8* R\$: 300.000,00		R\$: 2.400.000,00		
Item nº 04				300* R\$: 2.000,00		R\$: 600.000,00		
Item nº 05				3* R\$: 90.000,00		R\$: 270.000,00		
Item nº 06				12* R\$: 7.983,33		R\$: 95.799,96		
Item nº 07				0* R\$ 25.000,00		R\$:00,00		

TOTAL ORÇADO PARA O QUANTITATIVO MÍNIMO:		R\$: 7.262.164,97
CÁLCULOS COM QUANTITATIVOS MÁXIMOS		
Item nº 01	24.682 * R\$: 227,72	R\$: 5.620.585,04
Item nº 02	450.000 * R\$: 6,00	R\$: 2.700.000,00
Item nº 03	12 * R\$: 300.000,00	R\$: 3.600.000,00
Item nº 04	750 * R\$: 2.000,00	R\$: 1.500.000,00
Item nº 05	6 * R\$: 90.000,00	R\$: 540.000,00
Item nº 06	12 * R\$: 7.983,33	R\$: 95.799,96
Item nº 07	4 * R\$ 25.000,00	R\$: 100.000,00
TOTAL ORÇADO PARA O QUANTITATIVO MÁXIMO:		R\$: 14.156.385,00

13.3. Sobre a forma de efetivação do pagamento, ressalta-se que a prática do mercado em relação ao formato de pagamento anual das subscrições de softwares em licitações públicas é uma realidade cada vez mais comum no Brasil, impulsionada pela migração do modelo tradicional de aquisição de licenças perpétuas para o modelo de Software as a Service (SaaS).

13.4. A prática de mercado do pagamento anual antecipado (ou *upfront*) de subscrições de software é extremamente comum e consolidada, especialmente no modelo *Software as a Service* e na comercialização de licenças de grandes players de tecnologia. Desta forma, resta atendido o previsto no §1º do Art. 145 da Lei 14.133, representando esta prática de mercado, condição indispensável para a obtenção do bem ou para a prestação do serviço

13.5. O conceito de pagamento antecipado implica que o valor seja pago antes da ocorrência do fato gerador da obrigação da Administração, que é o adimplemento da obrigação por parte do contratado, ou seja, a entrega do bem ou a conclusão do serviço.

13.6. Embora no caso do presente processo haja certo alinhamento com o acima disposto, ou seja, com o pagamento integral das licenças sendo efetuado após a suas instalações e disponibilizações, para incremento da segurança da Administração, sugere-se pela edição e manutenção do tópico do modelo padronizado de Termo de Referência que versa sobre a antecipação de pagamento, condicionando que o contratado fica obrigado a devolver, com correção monetária, a integralidade do valor antecipado na hipótese de inexecução do objeto em caso de inexecução total, ou no caso de inexecução parcial, deverá haver a devolução do valor relativo à parcela não-executada do contrato.

14. Justificativa técnica da escolha da solução

14.1. Conforme fartamente demonstrado no tópico 9 do presente estudo técnico (análise comparativa de soluções), combinado com o exposto no tópico 11 (Análise comparativa de custos (TCO), a solução da TrendMicro foi a única que restou viável, uma vez que as demais soluções não atendem plenamente aos requisitos preestabelecidos.

14.2. Adicionalmente, registra-se que a contratação pretendida alinha-se à prestação de serviço e não mera aquisição de bem, pois além da obtenção das licenças, haverá prestação de serviços, a exemplo de instalação, atualizações contínuas de definições de vírus e suporte técnico.

14.3. Salienta-se também, a que a Equipe de Planejamento da Contratação observou, considerou e aplicou, quando cabível, as disposições trazidas no capítulo 1 Anexo I da In SGD/ME 94/2022 durante o levantamento das possíveis soluções, bem como na Elaboração do presente ETP, bem como que, pelas características inatas da solução a ser contratada, evidencia-se que a mesma não se enquadra nas vedações trazidas nos Arts. 4º e 5º da IN SGD/ME 94 /2022.

15. Justificativa econômica da escolha da solução

15.1 A presente contratação visa atender à necessidade de garantir a segurança da informação no ambiente corporativo institucional, mediante a aquisição de solução antivírus com tecnologia reconhecida no mercado, com funcionalidades avançadas de proteção, como inteligência artificial, detecção proativa e resposta automatizada contra ameaças cibernéticas. Para tanto, propõe-se a aquisição da solução Trend Micro, cujos benefícios técnicos e econômicos justificam a escolha.

15.2. Sob a ótica econômica, a aquisição da solução se justifica por representar uma alternativa viável e vantajosa em relação aos custos evitados com incidentes de segurança, como infecções por ransomware, vazamentos de dados e paralisações operacionais. Tais eventos podem gerar não apenas prejuízos financeiros diretos, mas também implicações legais, conforme previsto na Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), que impõe obrigações rigorosas quanto à segurança e integridade dos dados pessoais tratados pela Administração Pública.

15.3. Nesse sentido, a aquisição da solução Trend Micro contribui para:

- **Redução de custos com suporte corretivo** e recuperação de dados;
- **Prevenção de despesas não previstas** com resposta a incidentes e contratação emergencial de serviços de remediação;
- **Aumento da previsibilidade orçamentária**, mediante licenciamento centralizado e gestão integrada de endpoints;
- **Atendimento a requisitos legais e normativos** (LGPD, E-Ciber/CGU, normas internas de segurança da informação);
- **Redução do risco reputacional e institucional**, com proteção proativa contra ameaças avançadas.

15.4. Ressalta-se ainda que a padronização da solução de segurança proporciona ganhos de escala e economia operacional, reduzindo o tempo de resposta a incidentes, o retrabalho de equipes técnicas e os custos com treinamento, ao centralizar e unificar os procedimentos de gestão de segurança.

15.5. Dessa forma, a contratação da solução antivírus Trend Micro se revela tecnicamente adequada, economicamente vantajosa e alinhada às diretrizes legais e estratégicas de segurança da informação, constituindo medida preventiva e essencial à continuidade dos serviços públicos prestados pela PRF.

16. Benefícios a serem alcançados com a contratação

16.1. Fortalecimento da Segurança Cibernética Institucional

- Proteção em tempo real contra **malwares, ransomwares, trojans e ameaças zero-day**.
- Detecção e resposta automatizadas a ameaças avançadas.
- Monitoramento contínuo da integridade dos endpoints, servidores e ativos em nuvem.

16.2. Detecção e Resposta Estendida (XDR)

- Correlação de dados de múltiplas camadas (endpoint, e-mail, rede e nuvem).
- Visibilidade centralizada de ameaças em toda a infraestrutura da PRF.
- Resposta coordenada a incidentes com maior agilidade e precisão.

16.3. Redução da Superfície de Ataque

- Identificação e mitigação proativa de vulnerabilidades em estações e servidores.
- Controle de aplicações, portas, dispositivos e serviços expostos.
- Proteção de ambientes híbridos (on-premises + cloud).

16.4. Gerenciamento Centralizado e Escalável

- Console único para gestão de políticas de segurança em todo o território nacional.
- Instalação e atualização remota de agentes em milhares de hosts.
- Suporte a ambientes distribuídos, móveis e remotos.

16.5. Conformidade com Normativos de Segurança e LGPD

- Atendimento a requisitos da LGPD, e do Decreto nº 10.748/2021 (Estratégia Nacional de Segurança Cibernética).
- Geração de logs, relatórios e auditorias para prestação de contas e investigação.
- Apoio à governança de dados e proteção da privacidade.

16.6. Redução de Custos com Incidentes e Suporte

- Diminuição do número de incidentes causados por pragas virtuais.
- Redução de horas técnicas gastas com remediação manual.
- Menor impacto operacional causado por indisponibilidades.

16.7. Resposta Rápida e Automatizada a Incidentes

- Aplicação de playbooks automáticos para contenção de ameaças.
- Isolamento automático de máquinas infectadas.
- Aceleração no tempo médio de detecção e resposta.

16.8. Visibilidade e Inteligência de Ameaças

- Painéis analíticos com dados de risco por unidade, sistema e localidade.
- Priorização de vulnerabilidades com base em contexto e criticidade.
- Acesso à inteligência global de ameaças da Trend Micro.

16.9. Escalabilidade e Planejamento de Expansão

- Solução com arquitetura modular, permitindo ampliação conforme necessidades futuras.
- Capacidade de atender novas unidades, projetos ou requisitos legais sem mudança de plataforma.

17. Providências a serem Adotadas

17.1 Não há necessidade de adequação do ambiente para viabilizar a execução contratual (alínea "e", do art. 11, da Instrução Normativa SGD/ME nº 94/2022), uma vez que os sistemas da PRF suportam e atualmente já utilizam as soluções.

17.2 Considerando a complexidade, importância e sensibilidade em termos de segurança da informação e, ainda, considerando o valor envolvido na contratação em tela, importe que o Edital e seus anexos, tenham previsão de exigência de critérios de habilitação rigorosos.

17.3. A qualificação técnica serve para garantir que a empresa licitante tenha capacidade e experiência para entregar uma solução complexa e de alta criticidade, considerando que a segurança da informação de uma instituição policial é um pilar estratégico. Contratar uma empresa sem um histórico comprovado seria um risco enorme.

17.4 Adicionalmente, a previsão de critérios de habilitação técnica operacional conduz à contratação de empresa capaz de cumprir com aspectos como complexidade da solução descrita, tenha pessoal tecnicamente qualificado, goze de credibilidade e confiabilidade e possa fornecer adequado serviço de suporte e atualização.

17.5 Neste aspecto, é de extrema importância que a PRF preveja que a licitante interessada em contratar a solução apresente atestados de capacidade técnica que demonstrem que a empresa já prestou, com qualidade, serviços de complexidade tecnológica e operacional equivalente ou superior à do objeto desta contratação, de maneira a comprovar que a mesma tem capacidade técnica e operacional para manter a prestação do serviço de forma que não traga percalços ao órgão contratante.

17.6 A exigência de atestado com período mínimo de 12 (doze) meses fundamenta-se nos seguintes aspectos:

17.6.1. O objeto desta contratação consiste no fornecimento de licenças de uso com vigência anual, acompanhadas de suporte técnico contínuo durante todo o período contratual. Nesse contexto, a aceitação de atestados com duração inferior, ainda que somados, não demonstraria que a empresa possui experiência na execução e sustentação da solução ao longo de um contrato de médio prazo, limitando-se à atuação pontual ou de curto prazo.

17.6.2. A apresentação de múltiplos atestados de curta duração, a exemplo de fornecimentos mensais de licença e suporte ainda que hipoteticamente admitidos pelo mercado, não comprovaria a capacidade da empresa de manter a qualidade do serviço, o suporte técnico e a gestão da solução de forma contínua, ao longo de todo o ciclo de vigência contratual.

17.6.3. A exigência de experiência mínima de 12 (doze) meses evidencia que a licitante detém capacidade de planejamento, gestão contratual, suporte técnico continuado, atualização da solução e atendimento a demandas recorrentes, aspectos essenciais para contratos que envolvem licenciamento de software com suporte associado.

17.6.4. A comprovação de execução contínua por 12 (doze) meses constitui indicador objetivo de maturidade operacional, estabilidade organizacional e capacidade de sustentação da solução ao longo do tempo, atributos indispensáveis à adequada execução do objeto contratado.

17.6.5. Tal exigência mostra-se proporcional e razoável, uma vez que se limita a reproduzir, em termos de experiência pretérita, o próprio período de vigência da licença e do suporte ora contratados, não impondo ônus excessivo à competitividade, mas assegurando a seleção de licitante apta a cumprir integralmente o contrato.

17.5 Importante também prever exigência de comprovação de capacidade econômico financeira, visando garantir que a empresa possui condições financeiras sólidas para arcar com os custos e responsabilidades do contrato de valor elevado. A lógica é simples: um contrato desse valor tem uma execução de longo prazo e exige estabilidade do fornecedor.

17.6 Uma empresa financeiramente fraca pode ter dificuldade em cumprir com suas obrigações, como adquirir licenças, manter uma equipe dedicada ou até mesmo fornecer o suporte necessário ao longo do tempo. A exigência de indicadores como capital social, índices de liquidez e patrimônio líquido serve para mitigar esse risco.

17.7 Contratos de grande valor geralmente duram vários anos. A qualificação econômico-financeira garante que a empresa tem a robustez necessária para se manter no mercado e cumprir com suas obrigações durante toda a vigência do contrato. Isso evita que o órgão público precise fazer uma nova licitação no meio do caminho por conta da falência ou instabilidade financeira do contratado.

17.8 Exigir balanços e índices financeiros ajuda a filtrar empresas que não têm uma estrutura real e que podem participar da licitação apenas para tentar "vender" um serviço que não têm condições de entregar.

17.9 Importante também, caso a licitante não atinja os índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um), prever exigência de comprovação de capital mínimo em percentual a ser indicado no TR, visando assegurar que a empresa a ser contratada possua capacidade financeira suficiente para cumprir integralmente suas obrigações contratuais.

17.10 Considerando que a contratação abrange itens estratégicos e essenciais ao desempenho das atividades institucionais da PRF, mostra-se imprescindível assegurar que a contratada possua capacidade econômico-financeira compatível com o grau de responsabilidade e criticidade envolvido. A Administração, ao estabelecer tal patamar de exigência, busca dimensionar o requisito de forma proporcional e razoável, em consonância com a relevância do objeto contratado, de modo a mitigar riscos de inadimplemento e descontinuidade na execução, especialmente em cenários de maior complexidade operacional, riscos esses que não seriam adequadamente afastados por exigências menos robustas.

17.11 Sobre o critério de julgamento das propostas quando da definição da escolha do fornecedor a ser contratado, entende a equipe de Planejamento da Contratação que a opção pelo critério de menor preço é a mais adequada, para garantir que a administração pública consiga o melhor negócio possível para a solução. Vários fornecedores ou distribuidores podem vender os mesmos produtos da Trend Micro. A licitação com foco no menor preço incentivará a competição entre esses fornecedores, que buscarão oferecer o produto a um valor mais baixo para vencer o certame.

17.12 De outra banda, se a licitação fosse para a contratação de uma solução de segurança genérica, sem a especificação prévia do desenvolvedor, então a Administração poderia usar o critério de técnica e preço. Nesse caso, as empresas participantes teriam que apresentar suas soluções e seriam avaliadas tanto pela qualidade técnica da proposta quanto pelo preço, porém, como exposto o item anterior, não é o caso da presente contratação.

17.13. Considerando a importância e sensibilidade do objeto a ser contratado, para a devida robustez e segurança nos diversos aspectos envolvidos no ciclo de vida do contrato, é de suma importância que o Termo de Referência preveja que a empresa a ser contratada possua elevado nível de parceria com o desenvolvedor da solução.

17.14. Esta premissa refletirá em compromisso, volume de negócios, competências e especialização técnica do parceiro a ser contratado, garantindo a contratação de empresa que tenha um número mínimo de profissionais com certificações técnicas e de vendas ativas e capacidade de implementar soluções e prover o devido suporte com sucesso.

17.15. A exigência não se destina a restringir a competitividade do certame, mas sim a assegurar a capacidade técnica, a legitimidade da oferta e a adequada prestação de suporte durante a execução contratual.

17.16. Trata-se de contratação de solução de segurança da informação crítica, cuja eficácia depende diretamente do correto licenciamento, da atualização contínua de assinaturas, da rápida resposta a incidentes e do acesso a canais oficiais de suporte e escalonamento junto ao desenvolvedor.

17.17. A condição de parceiro certificado demonstra que o licitante possui autorização formal para comercializar a solução, acesso a recursos técnicos, atualizações, treinamentos e suporte especializado, mitigando riscos de fornecimento irregular, licenças inválidas ou indisponibilidade de atendimento em situações de criticidade.

17.18. Ressalte-se que a exigência não impõe exclusividade, tampouco restringe o certame a um único fornecedor, uma vez que os níveis de parceria indicados (Silver, Gold ou Platinum) correspondem às categorias ordinariamente disponibilizadas pelo próprio desenvolvedor ao mercado, acessíveis a múltiplos revendedores, desde que atendidos critérios objetivos previamente estabelecidos.

17.19. Ademais, a comprovação do vínculo é exigida no momento da apresentação da proposta, e não como condição prévia de participação, permitindo que potenciais licitantes regularizem sua condição junto ao desenvolvedor antes da contratação, o que preserva a ampla competitividade e a isonomia entre os concorrentes.

17.20. Cumpre acrescentar que, atualmente, a Contratante mantém a execução do serviço por meio de contrato em prorrogação excepcional, situação que, por sua própria natureza, é transitória e juridicamente sensível, demandando a adoção de medidas que assegurem a imediata continuidade do serviço tão logo concluído o procedimento licitatório.

17.21. Nesse contexto, a Administração pretende iniciar a execução do novo contrato de forma imediata após a conclusão da licitação, não havendo margem operacional para atrasos decorrentes de providências posteriores à adjudicação. Assim, embora a comprovação do vínculo de parceria com o desenvolvedor pudesse, em tese, ser exigida apenas na fase de contratação, optou-se por antecipar tal exigência para o momento da apresentação da proposta, considerando que os processos de certificação junto aos desenvolvedores não possuem prazo uniforme ou previsível, podendo eventualmente demandar tempo significativo, alheio à governança da Administração.

17.22. A antecipação da exigência tem por finalidade mitigar o risco concreto de descontinuidade de um serviço essencial de segurança da informação, cuja interrupção poderia expor a infraestrutura tecnológica da Polícia Rodoviária Federal a vulnerabilidades críticas, com impactos diretos na atividade-fim do órgão.

17.23. Trata-se, portanto, de medida preventiva, razoável e proporcional, diretamente vinculada à necessidade de garantir a pronta execução contratual, sem prejuízo à competitividade, uma vez que a certificação é condição ordinária de mercado para revendedores da solução.

17.24. Dessa forma, a exigência mostra-se necessária, proporcional e diretamente relacionada ao objeto contratado, atendendo aos princípios da razoabilidade, da segurança da informação, da eficiência administrativa e da seleção da proposta mais vantajosa, não se configurando como requisito restritivo ou desarrazoado.

18. Informações complementares

18.1. A natureza da solução de segurança da informação (antivírus) ora demandada apresenta caráter acessório e indissociável dos equipamentos de processamento de dados (desktops, notebooks e smartphones) utilizados pela Polícia Rodoviária Federal, constituindo-se como requisito mínimo para a operação segura desses ativos.

18.2. Em razão do dinamismo inerente à atividade policial, bem como dos ciclos contínuos de renovação, substituição e expansão do parque tecnológico do órgão, verifica-se a necessidade de ativações progressivas, contínuas e fracionadas ao longo do tempo, diretamente vinculadas ao ingresso de novos ativos de TI em operação.

18.2.1. Para atendimento dessa demanda variável e imprevisível, sem prejuízo à eficiência administrativa, optou-se pela realização de licitação convencional, com a contratação do quantitativo total estimado, porém com execução diferida, a ser materializada mediante a emissão de Ordens de Serviço, conforme a efetiva necessidade da Administração.

18.2.2. Tal modelagem confere maior previsibilidade orçamentária, assegura a disponibilidade da solução quando demandada e evita sucessivas contratações pontuais, que tenderiam a elevar custos transacionais e operacionais.

18.2.3. Embora o parcelamento do objeto constitua regra geral nas contratações públicas, a presente solução técnica recomenda a padronização e a gestão centralizada da contratação, tendo em vista a necessidade de uniformidade da solução de segurança, interoperabilidade, facilidade de gestão, resposta coordenada a incidentes cibernéticos e redução de riscos operacionais. A eventual fragmentação do objeto, especialmente

por meio da adoção do Sistema de Registro de Preços, implicaria a formação de múltiplos contratos ou instrumentos congêneres, com o mesmo fornecedor, o que acarretaria expressivo aumento da carga administrativa, gerando custos indiretos relevantes para a Administração.

18.2.4. Ademais, a gestão simultânea de múltiplos contratos de antivírus exigiria maior esforço de governança, acompanhamento de indicadores, controle de licenças, gestão de renovações e tratamento de incidentes, onerando indevidamente a estrutura administrativa e contrariando os princípios da eficiência, da economicidade e da racionalização dos meios.

18.2.5. Em consonância com o modelo de execução progressiva adotado, os requisitos de qualificação econômico-financeira e técnica serão dimensionados de forma proporcional às obrigações de execução imediata, notadamente aos quantitativos a serem ativados na assinatura contratual. Tal abordagem visa ampliar a competitividade do certame, evitando a imposição de exigências baseadas no volume total estimado, cuja execução ocorrerá de forma gradual e futura, que poderiam restringir indevidamente a participação de potenciais licitantes.

18.2.6. A medida alinha-se ao entendimento consolidado de que a qualificação deve ser estritamente necessária e suficiente ao cumprimento das obrigações efetivamente assumidas no momento inicial do contrato, em observância aos princípios da razoabilidade e da proporcionalidade.

18.3. Tratamento diferenciado para ME e EPP

18.3.1. Margem de preferência pela LEI COMPLEMENTAR Nº 123, DE 14 DE DEZEMBRO DE 2006.

18.3.1.1. Considerando que a estimativa do valor global da contratação é superior a R\$ 80.000,00 e considerando que o objeto está reunido de forma interdependente, de maneira que a adjudicação dar-se-à pelo menor valor global, não será aplicada a obrigatoriedade de contratação exclusiva para Microempresas e Empresas de Pequeno Porte (ME/EPP), nos termos do art. 48, I, da Lei Complementar nº 123, de 14 de dezembro de 2006. Ademais, a solução possui natureza indivisível, de modo que a sua fragmentação entre mais de um fornecedor não traria ganho de escala, podendo inclusive resultar em aumento de custos decorrente da necessidade de gerir mais de um contrato. Além disso, a divisão da contratação comprometeria a padronização e aumentaria o risco de inconsistências, informações conflitantes e indisponibilidades.

18.3.1.2. Nos termos do art. 4º, inciso I, da Lei nº 14.133/2021, as disposições constantes dos arts. 42 a 49 da Lei Complementar nº 123, de 14 de dezembro de 2006, não se aplicam a presente licitação, visto que o valor estimado ANUAL para o grupo é superior à receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.

18.3.2. Margem de preferência pelo DECRETO Nº 11.890, DE 22 DE JANEIRO DE 2024.

18.3.2.1. Considerando o Anexo I, da RESOLUÇÃO SEGES-CICS/MGI Nº 4, DE 18 DE OUTUBRO DE 2024, que regulamenta o Decreto nº 11.890/2024, que regulamenta o art. 26 da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre a aplicação da margem de preferência no âmbito da administração pública federal direta, autárquica e fundacional, e institui a Comissão Interministerial de Contratações Públicas para o Desenvolvimento Sustentável, observa-se a não aplicação da margem de preferência, uma vez que o serviço não está contido no rol da Resolução.

18.4. Classificação do objeto como atividade de execução indireta e de custeio

18.4.1. O objeto da presente contratação enquadra-se como atividade de execução indireta, nos termos do Decreto nº 9.507/2018, pois trata-se de um serviço de natureza auxiliar, sem vínculo com as atividades finalísticas da Polícia Rodoviária Federal. O objeto da presente contratação também enquadra-se como atividade de custeio, haja vista que se trata de atividade de suporte e despesa regular para manutenção do funcionamento da Administração Pública, conforme Capítulo II do Decreto 10.193/2019 e art. 2º, inciso II, da Portaria nº 7.828/2022/ME, sendo essencial para o pleno funcionamento das atividades institucionais da PRF.

18.5. Princípio da Padronização

18.5.1. O objeto da presente contratação segue o princípio da padronização previsto no Art. 40, V, a, da Lei 14.133/2021, na medida em que segue os modelos de artefatos padronizados da Advocacia Geral da União (AGU) e da Secretaria de Governo Digital (SGD), assim como toda regulamentação legal e infralegal aplicável do objeto.

18.5.2. Considerando Instrução Normativa nº 938/2022 da Secretaria de Gestão e Inovação do Ministério da Gestão e da Inovação em Serviços Públicos (SEGES/MGI), até o momento da finalização do presente Estudo Técnico, os únicos catálogos padronizados de contratação publicados pela referida Secretaria são referentes aos seguintes objetos: a) Água Mineral; b) Açúcar; e c) Café.

18.6. Vedação de consórcios

18.6.1. A participação de empresas em consórcio **não será permitida**, tendo em vista que o objeto da presente licitação consiste na aquisição de licenças de software antivírus, cuja execução não demanda a associação de empresas para garantir a capacidade técnica ou operacional. Tal vedação visa assegurar a celeridade, simplicidade e eficiência do processo licitatório, em consonância com os princípios que regem a modalidade pregão.

18.7. Não Parcelamento

18.7.1. O parcelamento da solução de TIC se mostrou tecnicamente inviável, pois as licenças, serviços de instalação, configuração, garantia e suporte do fabricante formam uma solução unificada.

18.7.2. É essencial que esses itens sejam fornecidos em conjunto, sem parcelamento, para garantir a implantação efetiva da solução.

18.7.3. Dessa forma, a contratação dos itens em um lote único assegura que todos os componentes sejam compatíveis entre si, garantindo a harmonia e o desempenho adequado da solução, além de promover maior facilidade na manutenção, suporte técnico e garantia, uma vez que todos os elementos estarão integrados e fornecidos por um único provedor.

18.8. A modalidade de contratação e de utilização da plataforma em análise, alinha-se com o conceito de utilização de software como um serviço contínuo, ultrapassando o conceito de "licenciamento de prateleira".

18.9. Adicionalmente, salienta-se que os serviços agregados ao fornecimento das licenças revelam que, diferentemente de um editor de texto, por exemplo, para garantir o desempenho esperado, uma solução de segurança depende de *feeds* de inteligência de ameaças em tempo real. Ainda, sem a atualização (update/upgrade) e o suporte, a solução torna-se inócua em poucos dias diante de novas vulnerabilidades. Também envolve atividade funcional de monitoramento e correlação de eventos que é, por natureza, uma prestação de serviço voltada à manutenção da infraestrutura computacional do órgão contratante.

18.10. Neste sentido, restam evidenciados para a presente contratação, a presença dos critérios da continuidade e essencialidade, e, por consequência, afastado o conceito de mera utilização de programa de informática, uma vez que, embora o tema de segurança cibernética seja considerada uma atividade acessória, ela é indispensável e de necessidade permanente para que o órgão não interrompa suas atividades.

18.11. Ante ao exposto nos subitens retro, entende-se que, sendo de interesse da alta gestão da área demandante, existe a possibilidade de aplicação do previsto no Art. 106 da Lei 14.133, permitindo que o Contrato possa ser renovado até o limite decenal, desde que as condições e os preços permaneçam vantajosos para a Administração.

19. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

19.1. Justificativa da Viabilidade

19.1. A futura contratação é viável visto que pode-se atestar a viabilidade técnica, administrativa e econômica para a sua execução.

20. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

Despacho: Integrante Técnico

ANDRE LUIZ DE SOUZA ARRUDA

Membro da comissão de contratação

Despacho: Integrante Administrativo

GIOVANI AUGUSTO TAGLIAPIETRA

Membro da comissão de contratação



Assinou eletronicamente em 19/03/2026 às 07:54:01.

Despacho: Integrante Requisitante

FABIO COVA MARTINS

Membro da comissão de contratação



Assinou eletronicamente em 19/03/2026 às 09:54:07.

Despacho: Autoridade máxima de TIC.

JOEDSON CAMILO DE OLIVEIRA

Autoridade máxima de TIC.



Assinou eletronicamente em 27/03/2026 às 14:03:17.

ISABEL IZAGUIRRE ZAMBROTTI DORIA

Equipe de apoio

Despacho: Integrante Técnico

EULER ARAUJO CHAVES NETO

Integrante técnico da EPC



Assinou eletronicamente em 19/03/2026 às 11:19:15.

Despacho: Autoridade Máxima de TIC substituto

ANDRE JORGE RAPOSO

Autoridade Máxima de TIC substituto