ESTUDO TÉCNICO PRELIMINAR – ETP

Processo Administrativo n. 16/2026
Solução de Proteção *Endpoints Detection and Response*

1. Introdução

As contratações governamentais produzem significativo impacto na atividade econômica, tendo em vista o volume de recursos envolvidos. Neste sentido, um planejamento bem elaborado propicia contratações potencialmente mais eficientes, posto que a realização de estudos previamente delineados conduz ao conhecimento de novas modelagens/metodologias ofertadas pelo mercado, resultando na melhor qualidade do gasto e em uma gestão eficiente dos recursos públicos.

A Lei n. 14.133, de 1° de abril de 2021, dispõe que a descrição da necessidade da contratação deve ser fundamentada em estudo técnico preliminar que caracterize o interesse público envolvido, dessa forma, o estudo técnico preliminar deverá evidenciar o problema a ser resolvido e a sua melhor solução, de modo a permitir a avaliação da viabilidade técnica e econômica da contratação.

2. Objeto

Contratação de empresa especializada para o fornecimento de solução de proteção de *endpoints* – antivírus de nova geração com funcionalidades de EDR – Endpoint Detection and Response.

3. Descrição da necessidade

A necessidade identificada decorre do aumento significativo da exposição dos ativos tecnológicos institucionais a ameaças cibernéticas sofisticadas, que superam a capacidade de resposta das soluções antivírus tradicionais. O cenário atual, marcado pela intensificação de ataques como *ransomware*, *phishing* direcionado e exploração de vulnerabilidades, exige a adoção de mecanismos avançados de defesa para garantir a integridade, confidencialidade e disponibilidade das informações sob responsabilidade institucional.

3.1. Detalhamento das necessidades identificadas

A solução corporativa de proteção de endpoints, com funcionalidades de EDR (*Endpoint Detection and Response*), é fundamental para ampliar a capacidade de prevenção, identificação proativa, investigação e resposta a incidentes de segurança em tempo real. Essa abordagem fortalece a proteção de estações de trabalho e servidores, mitigando riscos operacionais, financeiros e reputacionais decorrentes de incidentes cibernéticos.

Defesa Avançada: Necessidade de mecanismos que superem as limitações dos antivírus convencionais, proporcionando detecção e resposta automatizadas a ameaças emergentes.

Proteção Unificada: Demanda por solução que integre a proteção de diferentes dispositivos institucionais, promovendo a padronização e a eficiência operacional.

Suporte Técnico e Capacitação: Requisito de serviços de suporte, implantação, configuração e treinamento, assegurando a correta operacionalização da ferramenta e a internalização de boas práticas de segurança da informação.

Conformidade e Governança: Atendimento às diretrizes de governança e segurança da informação, alinhando-se às exigências normativas e à responsabilidade institucional.

3.2. Relação com o interesse público e estratégia da contratação

A adoção desta solução contribui para a continuidade e eficiência dos serviços públicos, protegendo informações estratégicas e ativos críticos institucionais.

A medida é adequada para garantir a proteção dos ativos de informação e a conformidade com as melhores práticas de governança e segurança da Administração Pública.

4. Requisitos da contratação

Para atender à necessidade de proteção avançada dos ativos tecnológicos institucionais diante das ameaças cibernéticas sofisticadas identificadas, é imprescindível que a solução a ser disponibilizada contemple requisitos essenciais em consonância com os normativos regentes e boas práticas de sustentabilidade. A seguir, são detalhados os requisitos mínimos necessários, bem como os marcos normativos aplicáveis e práticas de sustentabilidade relacionadas.

4.1. Requisitos necessários para o atendimento da demanda

4.1.1. Funcionalidade de EDR (*Endpoint Detection and Response*): Deve oferecer mecanismos de detecção, investigação proativa e resposta automatizada a ameaças em estações de trabalho e servidores, permitindo identificação em tempo real de atividades maliciosas, análise de comportamento e suporte a ações de remediação imediata.

4.1.2. Proteção Unificada de Diferentes Dispositivos: A solução deve possibilitar proteção centralizada de múltiplos tipos de dispositivos institucionais (estações de trabalho e servidores, físicos ou virtuais), assegurando cobertura uniforme e gestão eficiente a partir de console centralizada.
4.1.3. Compatibilidade com Ambiente Institucional: É necessário garantir compatibilidade com sistemas operacionais utilizados no parque tecnológico institucional e interoperabilidade com demais soluções de segurança em operação.

4.1.4. Capacidade de Atualização e Inteligência de Ameaças: A ferramenta deve manter-se constantemente atualizada mediante integração com feeds de inteligência de ameaças reconhecidos, possibilitando resposta ágil a ameaças emergentes.

4.1.5. Suporte Técnico Especializado: Deve ser garantida assistência técnica para implantação, configuração, operação e troubleshooting, com atendimento em idioma português e em regime compatível com a criticidade do serviço.

4.1.6. Capacitação e Transferência de Conhecimento: Inclusão de treinamento para equipes técnicas e usuários, promovendo capacitação acerca da utilização, operação e melhores práticas relacionadas à solução implementada.

4.1.7. Atendimentos a Normas de Governança e Segurança: Aderência às normas de segurança da informação, tais como ISO/IEC 27001 e 27002, bem como conformidade com marcos legais e normativos aplicáveis à Administração Pública.

4.1.8. Relatórios Gerenciais e Controle de Auditoria: Provisionamento de relatórios gerenciais, notificações de incidentes e logs de auditoria para acompanhamento, gestão e conformidade com os controles internos.

4.1.9. Conformidade com Políticas Institucionais: Alinhamento com as políticas e normativos internos de segurança e governança de TIC vigentes no órgão ou entidade demandante.

4.2. Normativos aplicáveis

4.2.1. Lei nº 14.133/2021 (Lei de Licitações e Contratos) – especial destaque para: Artigo 12: determina a necessidade de identificação clara dos requisitos para atendimento à demanda; Artigo 18: exige fundamentação técnica para o atendimento da necessidade.

4.2.2. Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD): estabelece princípios para tratamento adequado de dados pessoais, especialmente quanto à segurança da informação.

4.2.3. Instrução Normativa SGD/ME nº 1/2019: dispõe sobre governança de tecnologia da informação e comunicação na Administração Pública Federal direta, autárquica e fundacional.

4.2.4. Normas Técnicas Internacionais: recomenda-se conformidade com normas ISO/IEC 27001 (Sistemas de Gestão de Segurança da Informação) e ISO/IEC 27002 (Controles de Segurança).

4.3. Práticas de sustentabilidade

4.3.1. Ambiental: Incentivar a adoção de soluções que resultem em menor consumo energético, promovam virtualização e eficiente uso de recursos de hardware, bem como impeçam a necessidade de deslocamentos presenciais para atividades de treinamento e suporte, preferindo formatos digitais.

4.3.2. Econômica: Garantir que a solução ofereça ganhos de escala, padronização e redução de custos indiretos (como indisponibilidade de serviços e trabalho manual), alinhando-se aos princípios de economicidade e eficiência da administração pública.

Ao observar os requisitos acima e os normativos destacados, assegura-se a escolha de solução compatível com as necessidades institucionais, aderente às diretrizes legais, e fundamentada em práticas de responsabilidade ambiental e econômica. Tal abordagem fortalece a defesa dos ativos institucionais e a governança da informação perante os desafios contemporâneos de segurança cibernética.

5. Estimativa das quantidades a serem contratadas

Grupo	Produto/Item	Quantidade	CATSER	Valor Unitário Estimado	Valor Total Estimado
Lote único	Item 1: Solução de proteção *Endpoint Detection And Response* (EDR) em Nuvem com suporte técnico incluído	35 licenças de 3 anos (36 meses)	350949	R$ 773,95	R$ 27.088,25
	Item 2: Suporte técnico durante toda a vigência contratual				
	Item 3: Configuração e implantação	1	26972	R$ 3.096,67	R$ 3.096,67
	Item 4: Treinamento				
Valor Total Estimado da Contratação					**R$ 30.184,92**

6. Levantamento de mercado

6.1. Solução de EDR dedicada de classe corporativa (ex: Microsoft Defender for Endpoint, Crowdstrike Falcon, SentinelOne, Sophos Intercept X Advanced com EDR)

Essas soluções são líderes de mercado em proteção de endpoints, oferecendo mecanismos avançados de detecção, investigação, resposta automatizada e integração nativa com feeds de inteligência de ameaças. As plataformas fornecem console unificado, cobertura de múltiplos sistemas operacionais, integração com SIEMs, relatórios detalhados, autenticação multi-fator, automação de remediação e suporte técnico especializado em português.

Também permitem implantação flexível (on-premise, cloud ou híbrida), atingindo elevados padrões de compliance e governança (ISO/IEC 27001/27002, LGPD) e mantendo performance com uso racional de recursos computacionais. Estão alinhadas às necessidades de treinamentos e suporte e aderem a práticas de sustentabilidade (treinamentos remotos, uso eficiente de recursos, inclusão e diversidade nas equipes de projeto e suporte).

Pontos Positivos:

• Alta eficiência na detecção e resposta a ameaças em endpoints

• Console unificado com integração nativa a SIEMs e feeds de inteligência de ameaças

• Cobertura multiplataforma com flexibilidade de implantação (on-premise, cloud ou híbrida)
• Conformidade com normas de segurança e privacidade (ISO/IEC 27001/27002, LGPD)
• Suporte técnico especializado em português e opções de treinamentos remotos

Pontos Negativos:
• Custo elevado de licenciamento e manutenção anual
• Possível complexidade na implantação e gestão das soluções
• Dependência de internet para atualizações e algumas funcionalidades avançadas
• Necessidade de treinamento técnico especializado para operação efetiva
• Integração com sistemas legados pode apresentar desafios

6.2. Solução integrada de proteção de endpoint dentro de suíte UEM (Unified Endpoint Management) com EDR (ex: VMware Carbon Black + Workspace ONE, IBM Security MaaS360 com EDR)

Alternativa que une funcionalidades de EDR a recursos de gerenciamento unificado de endpoints, facilitando controle de políticas de segurança, inventário e compliance de dispositivos, especialmente em ambientes heterogêneos e amplamente distribuídos. Soluções UEM com EDR oferecem gerenciamento centralizado, automação de políticas, monitoramento comportamental, relatórios e integração com feeds de ameaças.

Possuem alta capacidade de customização, suporte a múltiplos sistemas operacionais, integração com políticas institucionais de TIC e ferramentas preexistentes, além de suporte em português, treinamentos para equipe e opções de implantação sustentável. Entretanto, apresentam níveis variáveis de profundidade na resposta a incidentes em comparação com plataformas EDR especializadas e, em geral, custos e complexidade maiores para implantação e integração total.

Pontos Positivos:
• Gerenciamento centralizado de dispositivos e políticas de segurança
• Automação de políticas de conformidade e relatórios detalhados
• Suporte a múltiplos sistemas operacionais e ambientes heterogêneos
• Integração com ferramentas institucionais preexistentes e feeds de ameaças
• Disponibilidade de suporte em português e opções de treinamento

Pontos Negativos:

• Complexidade elevada de implantação e integração

• Custos geralmente mais altos que soluções EDR isoladas

• Níveis variáveis de profundidade na resposta a incidentes

• Demandam maior capacitação da equipe técnica

• Possível sobreposição de funcionalidades em relação a ferramentas já existentes

6.3. Solução de Endpoint Protection Platform (EPP) aprimorada, combinando antivírus de nova geração com módulos adicionais de EDR (ex: Kaspersky Endpoint Security with EDR Optimum, Bitdefender GravityZone Elite, Trend Micro Apex One com EDR)

Plataformas EPP de próxima geração evoluíram para incorporar módulos de detecção e resposta estendida (EDR), agregando inteligência artificial e detecção comportamental à proteção tradicional de antivírus. Tais soluções atacam *ransomware*, *exploits* e ameaças persistentes avançadas, possibilitando investigação automatizada e manuais, criação de políticas centralizadas e integração de relatórios de conformidade.

Oferecem suporte especializado, são aderentes às melhores práticas de compliance, podem ser adquiridas via licenciamento por volume e são adaptáveis ao parque tecnológico preexistente. Costumam apresentar boa relação custo-benefício, porém, em alguns casos, os módulos de EDR dessas suites são menos robustos em relação a soluções EDR puras no tocante a resposta direta a incidentes mais sofisticados.

Pontos Positivos:

• Integração de antivírus de nova geração com capacidades de EDR em uma única solução

• Uso de inteligência artificial e detecção comportamental para ampliar a proteção contra ameaças avançadas

• Facilidade na administração centralizada de políticas e conformidade

• Adaptação a diversos ambientes e infraestrutura tecnológica já existente

• Boa relação custo-benefício e possibilidade de licenciamento por volume

Pontos Negativos:

• Módulos EDR integrados geralmente menos robustos que soluções EDR dedicadas

• Resposta a incidentes sofisticados pode ser limitada

• Dependência do fornecedor para atualizações e suporte especializado

• Possível complexidade na integração completa com algumas infraestruturas legadas

• Funcionalidades avançadas podem exigir custos adicionais ou módulos complementares

6.4. Alternativa Escolhida

Solução de EDR dedicada de classe corporativa (ex: Microsoft Defender for Endpoint, Crowdstrike Falcon, SentinelOne, Sophos Intercept X Advanced com EDR)

6.5. Justificativa

A solução de EDR dedicada de classe corporativa é a melhor alternativa considerando o cenário institucional, pois atende de forma completa todos os requisitos técnicos, normativos, de sustentabilidade e governança estipulados.

Esse tipo de solução é reconhecido por sua robustez na detecção e resposta proativa a ameaças sofisticadas que superam antivírus tradicionais, garante proteção unificada com alta capilaridade, integração com inteligência de ameaças, suporte técnico especializado em português, integração nativa com políticas e controles institucionais e práticas sustentáveis.

Além disso, apresenta elevada maturidade em relatórios gerenciais, conformidade com normas nacionais e internacionais de segurança da informação, suporte a treinamentos remotos, inclusão e racionalização de recursos. Essa abordagem maximiza o nível de proteção, reduz riscos operacionais, financeiros e reputacionais, contribui para a governança e fortalece a confiança institucional diante dos desafios contemporâneos da segurança cibernética.

7. Estimativa do preço da contratação

O valor total estimado para essa contratação é de R$ 27.088,25.

8. Descrição da solução como um todo

A opção selecionada para atender às necessidades institucionais é uma solução de EDR (*Endpoint Detection and Response*) dedicada de classe corporativa, exemplificada por ferramentas como Microsoft Defender for Endpoint, Crowdstrike Falcon, SentinelOne e Sophos Intercept X Advanced com EDR.

A escolha fundamenta-se na alta capacidade desse tipo de solução em proporcionar defesa avançada, resposta automatizada e gestão centralizada frente ao cenário crescente de ameaças cibernéticas, superando amplamente as capacidades dos antivírus tradicionais. A seguir, detalha-se como a solução escolhida responde integralmente às demandas técnicas, normativas e de sustentabilidade identificadas no estudo técnico preliminar.

8.1. Descrição Detalhada da Solução Escolhida

A solução de EDR dedicada de classe corporativa consiste em uma plataforma tecnológica específica para a proteção de endpoints (estações de trabalho e servidores), oferecendo recursos sofisticados para detecção proativa, investigação aprofundada e resposta automática a ataques cibernéticos de alta complexidade. Atua de forma integrada à infraestrutura institucional, com console centralizado e inteligência de ameaças em tempo real, suportada por suporte técnico diferenciado e alinhamento total a normativos e práticas de governança nacionais e internacionais.

Características Principais	Como a solução atende às necessidades
Funcionalidade avançada de EDR	Proporciona detecção em tempo real, investigação comportamental detalhada e automação de respostas a ameaças complexas como *ransomware*, *phishing* e *exploits*, superando limitações dos antivírus convencionais.
Proteção unificada e centralizada	Permite gestão de segurança de diferentes dispositivos (estações físicas, virtuais e servidores) a partir de um console único, padronizando operações e facilitando a administração centralizada.
Compatibilidade ampla	É compatível com múltiplos sistemas operacionais e possui integração nativa com demais soluções de segurança já existentes na instituição, preservando a interoperabilidade.
Atualização contínua e inteligência de ameaças	Integra-se a fontes reconhecidas de feeds de inteligência de ameaças mundiais, recebendo atualizações constantes e permitindo resposta ágil a novas vulnerabilidades e modalidades de ataque.
Suporte técnico especializado	Conta com assistência técnica altamente capacitada, atendimento em português e cobertura em regime compatível com a criticidade dos serviços institucionais, incluindo apoio à implantação, configuração e *troubleshooting*.
Capacitação e transferência de conhecimento	Prevê treinamentos remotos para a equipe técnica e usuários-chave, promovendo internalização de boas práticas, aumento da autonomia e elevação do nível de maturidade em segurança da informação.
Conformidade normativa e governança	Adere aos requisitos legais (Lei nº 14.133/2021, LGPD, E-Ciber), políticas internas e normas técnicas internacionais (ISO/IEC 27001/27002), fortalecendo a governança de TIC e mitigando riscos regulatórios.
Relatórios gerenciais	Oferece relatórios detalhados, logs de auditoria e notificações automatizadas, servindo como instrumento para controle interno, prestação de contas e suporte a auditorias e tomadas de decisão.
Alinhamento com políticas institucionais	Aderência e integração plena com normativos internos, políticas de TIC e diretrizes específicas da

	instituição, promovendo padronização, eficiência e compliance.

8.2. Diferenciais e benefícios da solução escolhida

Robustez Técnica: Destaca-se por sua capacidade de detectar, isolar e remediar ameaças sofisticadas rapidamente, reduzindo riscos operacionais e de indisponibilidade.

Eficiência Operacional: Consolida múltiplos controles e processos de segurança em um único ponto de gestão, otimizando recursos humanos e reduzindo redundâncias.

Governança e Conformidade: Facilita o cumprimento de obrigações legais, regulatórias e de auditoria, agregando transparência e rastreabilidade às ações de segurança.

Sustentabilidade e Inclusão: Promove práticas responsáveis, reduz custos indiretos com deslocamento e energia, e contribui para ambiente institucional mais diverso e ético.

Alinhamento Estratégico: O ingresso em iniciativas como a Intenção de Registro de Preços nº 03/2026 reforça a economicidade, a garantia de escala, a padronização tecnológica e a agilidade nos processos de contratação, em consonância com os interesses do serviço público.

8.3. Conclusão

Ao optar por uma solução de EDR dedicada de classe corporativa, a instituição assegura a máxima proteção dos ativos tecnológicos frente ao avanço das ameaças cibernéticas, além de atender de forma abrangente aos requisitos técnicos, regulatórios e de sustentabilidade. Essa solução fortalece a integridade, confidencialidade e disponibilidade da informação, promovendo resiliência cibernética e confiança institucional, e demonstrando compromisso com as melhores práticas e exigências legais contemporâneas no contexto da Administração Pública.

9. Viabilidade da contratação

A contratação mostra-se viável sob os aspectos técnico, econômico e jurídico.

Do ponto de vista técnico, a solução de EDR dedicada de classe corporativa atende integralmente aos requisitos definidos no presente estudo, oferecendo funcionalidades compatíveis com a complexidade das ameaças cibernéticas atuais, bem como aderência aos ambientes tecnológicos institucionais e às diretrizes de segurança da informação.

Sob o aspecto econômico, sublinhe-se que a estimativa de valor da contratação possui respaldo em contratações similares realizadas no âmbito da Administração Pública, evidenciando relação custo-benefício favorável e vantajosidade ao Conselho.

No que se refere ao aspecto jurídico, a contratação encontra amparo na Lei nº 14.133/2021, especialmente quanto à necessidade de planejamento e definição de requisitos, bem como na

Lei nº 13.709/2018, no tocante à adoção de medidas de segurança para proteção de dados pessoais, além de observar normas e boas práticas aplicáveis à governança de TIC.

Diante disso, conclui-se que a contratação é viável e adequada ao atendimento da necessidade identificada, não sendo constatados impedimentos à sua realização.

Vitória/ES, *data conforme assinatura eletrônica*.

Documento assinado digitalmente
gov.br
GUILHERME LUIZ LYRIO SIMONETTI
Data: 22/05/2026 11:13:44-0300
Verifique em https://validar.iti.gov.br

Guilherme Luiz Lyrio
Chefe da Tecnologia da Informação do Core-ES