Governo do Distrito Federal

Secretaria de Estado de Saúde do Distrito Federal

Gabinete

Coordenação Especial de Tecnologia de Informação em Saúde

Estudo Técnico Preliminar - SES/GAB/CTINF

1. INFORMAÇÕES BÁSICAS

Número do processo: 00060-00210274/2023-96

2. INTRODUÇÃO

O Estudo Técnico Preliminar é o documento que descreve as análises realizadas quanto às condições da contratação em termos de necessidades, resultados pretendidos, requisitos, alternativas, escolhas, custos e demais características, e que demonstra a viabilidade técnica e econômica da pretensão e integra a fase de Planejamento da Contratação, conforme regulamentado no Decreto n.º 44.330, de 16 de março de 2023, que Regulamenta a Lei Federal n.º 14.133, de 1º de abril de 2021, Lei de Licitações e Contratos Administrativos, no âmbito da Administração Pública direta, autárquica e fundacional do Distrito Federal e na Instrução Normativa SGD/ME n.º 94, de 23 de dezembro de 2022, a qual dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal, visto que, conforme termos do Decreto n.º 45.011, de 27 de setembro de 2023, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação (TIC) pelos órgãos e entidades da Administração Direta e Indireta do Distrito Federal, ocorreu a adoção da regulamentação editada pela União sobre as contratações de bens e serviços de tecnologia da informação no âmbito da Administração Pública Direta e Indireta do Distrito Federal.

Em sentido geral, a necessidade de realizar estudos técnicos preliminares, como etapa fundamental do planejamento de uma contratação, decorre antes de tudo dos princípios consagrados no art. 37 da Constituição Federal:

> (...)
> Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade,
> publicidade e eficiência [...] (BRASIL, 1988).
> (...)

Eficiência pode ser entendida como a maximização da capacidade dos recursos disponíveis, isto é, obter o melhor resultado com menos recursos, visando qualificar o gasto público sem se descuidar dos demais princípios constitucionais.

Assim, no presente documento, os Integrantes Técnicos e Requisitantes da Equipe de Planejamento da Contratação, ora designados pela Ordem de Serviço n.º 5, de 19 de janeiro de 2024, publicada no Diário Oficial do Distrito Federal n.º 16, de 23 de janeiro de 2024, considerando o conteúdo mínimo prescrito no art. 11 da IN SGD/ME n.º 94/2022 e as demais referências legais e normativas aplicadas às compras públicas e, especificamente, às aquisições de Tecnologia da Informação e Comunicação, dedicaram-se a analisar aspectos fundamentais relacionados à demanda em questão, tais como: adequação técnica; funcionalidades e requisitos; adequação às normas vigentes; modelos de execução; capacidade do mercado; estimativa preliminar de custos e viabilidade econômico-financeira do objeto.

3. DESCRIÇÃO DA NECESSIDADE

Trata-se de demanda formulada pela Gerência de Atendimento (GEAT), da Diretoria de Governança de Tecnologia da Informação (DGTI), desta CTINF, a qual requer, através do Documento de Formalização de Demanda (131365999), a contratação de solução de segurança da informação e comunicação.

Em análise da demanda, constata-se que devido a missão institucional da SES-DF, há a necessidade de uma grande estrutura assistencial e de vigilância em saúde a fim de prover serviços com níveis de excelência e em caráter ininterrupto para a boa e regular realização e condução das suas atividades. Em decorrência disso, necessita de uma grande estrutura assistencial e de vigilância em saúde a fim de prover serviços com níveis de excelência e em caráter ininterrupto para a boa e regular realização e condução das suas atividades.

Atualmente, essa estrutura assistencial e de vigilância em saúde é composta por mais de 300 (trezentos) estabelecimentos de saúde, as quais são procuradas cotidianamente pela população do Distrito Federal, em busca de serviços assistências e insumos para saúde.

Tendo em vista a informatização das unidades assistenciais, ocorrida ao longo dos anos, esta SES-DF dispõe de um parque computacional de mais de 15.000 (quinze mil) computadores, em volume estimados, os quais são utilizados de forma ininterrupta para efetuar registros em saúde, dispensação de insumos para saúde, bem como para a consecução das atividades administrativas de rotina e urgência do órgão.

Como consequência, há contínua e elevada troca de informações eletrônicas com grande e complexo volume de dados, os quais requerem proteção permanente visando assegurar a confiabilidade, disponibilidade e integridade dos dados e informações do órgão, ou àquelas sob sua custódia.

A proteção e segurança das informações em uma organização de grande porte, complexa e robusta, como é o caso da SES-DF, depende da adoção e manutenção de estratégias e tecnologias voltadas para a identificação e bloqueio de ameaças, tratamento e monitoramento de vulnerabilidades, bem como para a descoberta de eventos de comprometimento da segurança e resposta aos incidentes de segurança.

No cenário atual, as ameaças cibernéticas são crescentes e apresentam elevado grau de sofisticação, exigindo ações efetivas de prevenção e combate às práticas maliciosas, as quais podem comprometer em caráter definitivo e de forma irrecuperável o ambiente tecnológico do órgão, capturando dados, causando indisponibilidade e comprometendo a confiabilidade de sistemas, bem como a integridade dos equipamentos computacionais. Dentre as principais fontes de contaminação por pragas digitais e ataques cibernéticos estão, respectivamente, os dispositivos portáteis infectados com códigos maliciosos e o acesso à Internet.

Diante disso, urge compulsória do emprego de recursos de tecnologia da informação específicos, que abarque as mais recentes funcionalidades no que tange a detecção, bloqueio, investigação e resposta a incidentes de segurança da informação que venham porventura ocorrer no âmbito desta Secretaria.

Em linhas gerais a necessidade limitar-se-á:

a) Implementação de solução de segurança do tipo *endpoint* para prevenção, detecção, investigação e resposta a incidentes de segurança da informação.

Portanto, a pretensa contratação visa prover o órgão com uma solução de Tecnologia da Informação e Comunicação (TIC) para a prevenção contra intrusões e vazamentos de dados, detecção de vulnerabilidades e resposta em tempo hábil à ameaças cibernéticas e incidentes de segurança da informação.

3.1. Análise do cenário atual

Atualmente, para proteção, detecção, investigação e resposta a incidentes de segurança da informação, a SES-DF utiliza-se primordialmente a solução de *software Windowns Defender Antivírus,* na versão gratuita. Essa solução é pré-instalada no sistema operacional *Windows,* versões 10 e 11, para fins de proteção do ponto de extremidade.

O Windows Defender é um antivírus básico que oferece recursos como verificação de disco rígido atrás de infecções, além de detecção em tempo real e remoção de malwares. Embora seja funcional e totalmente integrado ao sistema operacional, essa solução apresenta algumas limitações, que incluem a falta de proteção contra *ransomware, firewall* pessoal, proteção contra *phishing* e detecção de comportamento malicioso. Ainda, constata-se a ausência de recursos de gerenciamento centralizado, atualizações de definição frequentes e suporte técnico.

Em decorrência disso, identificamos dois problemas principais, o primeiro relacionado à possibilidade de contaminação do parque computacional por pragas digitais, as quais dado o elevado nível de sofisticação podem contaminar e comprometer em caráter definitivo e de forma irrecuperável o ambiente tecnológico do órgão, capturando dados, causando indisponibilidade e comprometendo a confiabilidade de sistemas, bem como a integridade dos equipamentos computacionais.

Já o segundo relaciona-se à incapacidade de atuar preventivamente na identificação e bloqueio de ameaças, tratamento e monitoramento de vulnerabilidades, bem como na descoberta de eventos de comprometimento da segurança e resposta aos incidentes de segurança.

Tendo em vista a criticidade dos dados transitados cotidianamente no ambiente computacional desta Secretaria, os quais são originados da execução dos serviços assistências, muitas das quais são invioláveis, pois estão ligados a intimidade, a vida privada, a honra e a imagem das pessoas, há preocupação adicional com o nível de segurança que deve ser estabelecido para assegurar a confiabilidade, disponibilidade e integridade desses.

Diante disso, como forma de preservar o valor que os dados possuem para a organização, faz se necessário o emprego de uma solução de tecnologia da Informação e comunicação robusta, que ofereça camadas de segurança contra ameaças básicas e avançadas, baseadas em comportamento e inteligência artificial, capazes de detectar anomalias na execução de processos e operações, assim como oferecer instrumentos para investigação da causa raiz do problema, de maneira a proteger o ambiente de novos ataques.

Além disso, no sentido de garantir a confidencialidade, integridade e disponibilidade das informações, impedindo que eventos críticos comprometam a veracidade delas, é essencial que políticas e procedimentos de segurança sejam estabelecidos e implementados de forma permanente e evolutiva.

Outrossim, é primordial aprimorar a atuação preventiva, elevar o grau de detecção de comportamentos anômalos e desenvolver o processo de gestão de incidentes de segurança, agilizando a adoção de ações de contramedida de segurança e melhorando a percepção de segurança perante os usuários internos e à sociedade.

Tais medidas são fundamentais para manter e assegurar a disponibilidade adequada dos serviços de TI, em casos de tentativa de exploração de vulnerabilidade, além de permitir a continuidade das operações, apoiando os demais setores desta Secretaria de forma a manter seus dados íntegros, seguros e disponíveis.

Com a finalidade de compreender o cenário de vulnerabilidade, os registros de reclamações e indicações de ataques de vírus ao parque computacional da SES-DF, foi solicitado à Gerência de Projetos e Suporte (GPROS), por meio do processo SEI 00060-00519792/2023-72, Memorando Nº 182/2023 - SES/GAB/CTINF (125263562), o histórico de incidentes relacionados a ataques diretos a *endpoints* e em massa.

Como resposta, obtivemos a informação que não há registro contábil dessas ocorrências, uma vez que não possuímos ferramenta informatizada para detecção de *vírus*, *phishing*, *malware, ransonware,* entre outras pragas digitais. Quanto a ataques em massa, no foi informado que no ano de 2022 ocorreu uma disseminação de pragas digitais no Hospital Regional de Sobradinho (HRS), afetando aproximadamente 60 (sessenta) máquinas, circunstância que paralisou os serviços de TI naquele em parte daquele estabelecimento de saúde.

Adicionalmente, àquela unidade setorial acostou nos autos os relatórios (125734060 e 125734975), produzidos sem ônus pelas empresas OREV System, em 2021, e StyxGuard, em 2022, respectivamente, prestadores de serviços do segmento de segurança da informação, cujos resultados revelam a gravidade das condições de segurança da rede de dados desta Secretaria.

No mais, não podemos deixar de citar o episódio de segurança ocorrido no ano de 2017, quando da disseminação do vírus *Anacrai*, que paralisou os sistemas de saúde desta Secretaria.

Desta forma, em razão dos fatos relatados, a contratação em tela se revela indispensável à proteção dos dados e informações do órgão, permitindo assim que o órgão continue cumprindo com seu papel institucional de provedor serviços assistências com níveis de excelência e em caráter ininterrupto à população do Distrito Federal.

4. ÁREA REQUISITANTE

Área Requisitante: Gerência de Atendimento (GEAT)

Responsável: Fábio Ayub Brasil

5. NECESSIDADES DE NEGÓCIO

As necessidades de negócio envolvidas na pretensa contratação em estudo representam o detalhamento do objeto a ser contratado, O QUE a solução deve prover, independentemente da tecnologia que se empregue ou dos padrões tecnológicos da Instituição.

Nesse contexto, a solução deve atender às seguintes exigências:

a) Proteção contra ameaças digitais, com funcionalidades de detecção, bloqueio, investigação e resposta a incidentes;

b) Detecção de anomalias na execução de processos e operações;

c) Detecção, monitoramento e tratamento de vulnerabilidades;

d) Salvaguarda dos ativos de tecnologia da informação;

e) Continuidade dos processos de negócios;

f) S*oftwares* em língua escrita e falada em português do Brasil (pt-BR), com exceção de termos técnicos usuais que poderão ser apresentados em língua estrangeira.

6. NECESSIDADES TECNOLÓGICAS

As necessidades tecnológicas definem os padrões, metodologias, processos definidos, competências das equipes, entre outros aspectos, que a solução deve atender para que atinja o desempenho e os resultados esperados.

Nesse contexto, a solução deve atender às seguintes exigências:

a) Console de gerenciamento centralizado, acessível por meio de interface baseada na Web, mediante credencial de segurança, previamente definida;

b) A solução deve manter log de auditoria com registro das configurações realizadas por qualquer usuário ou administradores da solução;

c) A solução deve ser compatível com o sistema operacional Windows 10 ou superior, arquitetura 32 e 64 bits;

d) A solução deverá incorporar técnicas de aprendizado de máquina (*Machine Learning*) para detecção e prevenção de ataques.

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

São requisitos mínimos necessários à escolha da solução de TIC, aqui consideradas como premissas da área requisitante:

a) Provimento de atualizações da base de dados (lista de vírus e vacinas).

8. ESTIMATIVA DE VOLUME DE BENS E SERVIÇOS

Para realizar o dimensionamento do volume estimado de bens e serviços, preliminarmente foi considerada a quantidade estimada de microcomputadores do tipo desktop e portátil, no parque computacional da Secretaria, uma vez que a licença que se pretende contratar é instalada e vincula-se a esse dispositivo final, assim como a quantidade de servidores virtuais utilizados.

Tabela 1 - Estimado de bens e serviços.

Id.	Descrição	Processo SEI	Quantidade Total
1	Microcomputadores do tipo desktop.	00060-00357472/2020-70	7.594
2	Microcomputadores do tipo desktop.	00060-00180255/2023-28	7.220
3	Servidores virtuais	00060-00519792/2023-72	78
Total			**14.882**

Consideramos pertinente registrar que não identificamos processo de aquisição de microcomputadores do tipo portátil e *tablet*, no âmbito da SES-DF. Portanto, eventuais equipamentos dessa natureza, se incorporados ao acervo patrimonial da SES-DF, foram originados em processo de doação.

Por fim, visando atender as demandas porvindouras por novas licenças de *software antivírus* decorrente da ampliação da prestação de serviços à Sociedade, por meio da abertura de novos estabelecimentos de saúde e/ou pela ampliação dos existentes, bem pela incidência de demanda não mapeadas, será estabelecida margem de segurança de 10% (dez por cento). Portanto, temos a seguinte quantidade estimada:

Tabela 2 - Estimado de bens e serviços.

Id.	Descrição	Unidade	Quantidade	Margem de Segurança (+10%)	Quantidade Total
1	Solução de Segurança da Informação.	Licença por dispositivo	14.892	1.489	16.381

Isso posto, consideramos pertinente registrar as seguintes restrições técnicas ao pleno mapeamento das demandas por *software* antivírus:

a) Há uma gama de equipamentos originários de doação os quais ainda permanecem conectados à rede de dados.

9. LEVANTAMENTO DE SOLUÇÕES

O levantamento de soluções, nos termos da letra b, do inciso II do art. 11 da IN SGD/ME n.º 94/2022, visa a identificar alternativas para atendimento da demanda. Dentre as opções mercadológicas disponíveis, identificamos as seguintes soluções:

Tabela 3 - Levantamento de soluções.

Id.	Descrição da Solução
1	Solução de segurança do tipo antivírus livre ou gratuito.
2	Solução de segurança do tipo antivírus licenciado.
3	Solução de segurança do tipo detecção e resposta.
4	Solução de segurança do tipo detecção e resposta estendida.

10. ANÁLISE COMPARATIVA DAS SOLUÇÕES

A análise comparativa de soluções, nos termos do inciso II do art. 11 da IN SGD/ME n.º 94/2022, visa analisar as alternativas para atendimento da demanda considerando os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

10.1. Solução 1: Solução de segurança do tipo antivírus livre ou gratuito.

Esta solução consiste na utilização de *softwares* livres, projetados para detectar, impedir e remover códigos maliciosos, vírus, *worms, trojans, spyware, adware* e outros tipos de ameaças de um sistema de microcomputadores. Esse *software* depende de atualizações e vacinas, que devem ser desenvolvidas contra os novos tipos de malware. A versão destinada à área comercial é licenciada gratuitamente.

Entendemos que este cenário apresenta as seguintes vantagens:

- Menor dependência do fornecedor da solução; e
- Ausência de investimentos no licenciamento da solução.

Entendemos que este cenário apresenta as seguintes desvantagens:

- Limitações de funcionalidades;
- Ausência de garantia de atualização;
- Ausência de suporte técnico do fabricante;
- Dependência da comunidade desenvolvedora para a disponibilidade de novas funcionalidades e vacinas; e

- Necessidade de corpo técnico dedicado e capacitado para realizar o suporte técnico e gestão dos incidentes.

A utilização de *softwares antivírus* gratuitos disponíveis na internet apresenta poucas vantagens, as quais se limitam a menor dependência do fornecedor da solução e ausência de custos de licenciamento. Essa solução, possibilita a implementação de uma infraestrutura baseada em soluções de software livre, como respectivamente AVG ou Bitdefender, Postifix. Estas plataformas abertas podem ser consideradas o motor ou o coração de grande parte das soluções de segurança, já que delas derivam a maioria das ferramentas de mercado hoje disponíveis, inclusive proprietárias.

Ainda assim, mesmo servindo de base para diversas outras soluções, projetos ou produtos complementares a estas plataformas livres se fazem necessários devido à pouca ou baixa facilidade de operação destes softwares, com os quais a interação é realizada prioritariamente através de linhas de comando. Este tipo de interface, apesar de oferecer uma flexibilidade e versatilidade praticamente ilimitada, torna a gestão da solução mais propensa a erros humanos e demanda um nível de conhecimento bastante mais elevado dos profissionais que as operam, consequentemente tornando a administração destas soluções mais onerosa.

Há que se considerar, no entanto, que estas soluções são implementações em software, e têm como requisito a existência de uma plataforma em hardware para serem executadas. Ou seja, apesar de serem gratuitas, inclusive para uso corporativo, não eximem o Órgão de adquirir equipamentos necessários para a implementação de sua infraestrutura.

Também traz um ônus operacional bem maior à solução, pois toda a implementação deverá correr a cargo do corpo técnico da SES-DF, o qual possui sérias limitações qualitativas e quantitativas.

É importante também ressaltar que estas plataformas possuem restrições de funcionalidades essenciais para a SES-DF, como não estender suas funcionalidades à gestão do parque. Ou seja, a adoção de qualquer das soluções mencionadas neste cenário demandaria a utilização de outra ferramenta para gerenciar os dispositivos finais ou, no pior caso, a configuração individual de cada equipamento da SES-DF.

Este cenário pode ser uma alternativa viável num contexto em que se tenha um número reduzido de equipamentos, mas se torna excessivamente oneroso em um ambiente como o da SES-DF, com cerca de 15.000 dispositivos ativos e frente à escassa mão de obra disponível.

Ainda, que atualizações de software livre dependem das comunidades desenvolvedoras, não existindo uma formalização de contrato que possibilite responsabilização por descumprimento de níveis de serviço frente a tempestividade a resposta e implantação da solução aos ataques sofridos.

Diante disso, em razão dos fatos relatados, a presente solução **demonstra ser tecnicamente inviável**.

10.2. Solução 2: Solução de segurança do tipo antivírus licenciado.

Esta solução consiste na utilização de um *software* projetado para detectar, impedir e remover códigos maliciosos, vírus, *worms, trojans, spyware, adware* e outros tipos de ameaças em microcomputadores. Esse *software* depende de atualizações e vacinas, que devem ser desenvolvidas contra os novos tipos de malware. A versão destinada à área comercial é licenciada na forma de subscrição por dispositivo.

Entendemos que este cenário apresenta as seguintes vantagens:

- Proteção contra vírus, *spyware e spam*,
- Proteção das informações na Web;
- Custos baixos;
- Solução conhecida pelo corpo técnico.

Entendemos que este cenário apresenta as seguintes desvantagens:

- Oferece apenas o nível de proteção básicas nos dispositivos finais;
- Possui técnicas limitadas de detecção de vírus e intrusão;
- Ausência de gerenciamento centralizado;
- Adota uma abordagem reativa;
- Não detecta ameaças modernas que não introduzem novos arquivos no sistema; e
- Necessidade de corpo técnico dedicado e capacitado para gestão dos incidentes de forma local, ou seja, em cada dispositivo final.

A solução de antivírus tradicional concentra-se em combater ameaças baseadas em arquivos de assinatura ou definição, ou seja, essa solução combate às ameaças digitais exploradas, identificadas e documentadas. Não conseguindo, portanto, detectar ameaças modernas que não introduzem novos arquivos no sistema, como por exemplo: ataques baseados em memória, linguagem de script do PowerShell, logins remotos, ou que ainda não foram exploradas, identificadas e documentadas, como o ataque zero-day.

Logo, a tecnologia utilizada por antivírus tradicionais está ultrapassada, não fazendo frente às novas formas de atividades intrusivas, decorrente do rápido avanço de informações através da Internet, circunstância que aumentou a possibilidade de vulnerabilidades dos órgãos e instituições.

Diante disso, em razão dos fatos relatados, a presente solução **demonstra ser tecnicamente inviável**.

10.3. Solução 3: Solução de segurança do tipo detecção e resposta.

Esta solução é uma abordagem integrada e em camadas para proteção de *endpoint* (dispositivos finais), baseada em agente com funcionalidade de *Endpoint Detection and Response* (EDR). O EDR combina monitoramento contínuo em tempo real, coleta de dados e correlação avançada para detectar e responder a atividades suspeitas em conexões de *host* e *endpoint*. Essa abordagem permite que as equipes de segurança identifiquem e correlacionem rapidamente as atividades para produzir detecções de alta confiança com opções de resposta manuais e automatizadas. A versão destinada à área comercial é geralmente licenciada na forma de subscrição por dispositivo, por meio de soluções baseadas em nuvem.

Entendemos que este cenário apresenta as seguintes vantagens:

- Monitoramento contínuo, de forma centralizada, em tempo real dos agentes instalado nos *endpoints*;
- Facilidade na correlação avançada para detectar e responder a atividades suspeitas;
- Detecção e rastreio de movimentos de ameaças potenciais no ambiente;
- Detecção de arquivos e ações maliciosas baseado em comportamento;
- Detecção de scripts e comandos mal-intencionados a partir de *playbooks* e padrões de execução;
- Detecção de ataques do tipo "*Live off the Land*";
- Ampla camada de visibilidade quanto ao status de *endpoints* em relação a atividades maliciosas;

- Registro de eventos e qualificação daqueles que de fato precisam ser analisados;
- Ampla camada investigativa, através de coletas de evidências para análise forense;
- Proteção nas camadas de e-mail, rede e dispositivos finais;
- Estabelecimento de um framework eficiente para resposta a incidentes de segurança; e
- Execução de arquivos em *sandbox* para detecção de "zero day".

Entendemos que este cenário apresenta as seguintes desvantagens:

- Custos mais elevados quando comparado com uma solução de antivírus tradicional;
- Necessidade de hardware robusto para suportar as atividades de monitoramento contínuo, coleta e análise de dados; e
- Necessidade de corpo técnico dedicado e capacitado para análise e interpretação dos dados coletados.

A solução de segurança do tipo detecção e resposta apresenta uma nova abordagem de detecção e prevenção de ameaças, com tecnologia de aprendizado de máquina e de inteligência artificial, que auxiliam na identificação de padrões de comportamento fraudulento em meio à utilização convencional dos recursos tecnológicos.

A solução se concentra em eventos (arquivos, processos, aplicativos e conexões de rede) para observar como as ações ou os fluxos de eventos em cada uma dessas áreas estão relacionados. A análise de fluxos de eventos pode ajudar a identificar comportamentos e atividades maliciosas e, uma vez identificados, os invasores podem ser bloqueados.

Diante disso, em razão dos fatos relatados, a presente solução **demonstra ser tecnicamente viável**.

10.4. Solução 4: Solução de segurança do tipo detecção e resposta estendida.

Esta solução é uma abordagem de detecção e resposta estendida (*Extended Detection and Response* - XDR), baseada em SaaS, específica do fornecedor, que nativamente integra vários produtos de segurança em um sistema para a detecção, investigação e resposta em várias camadas de segurança. O XDR desfaz silos de segurança para identificar toda a trajetória de um ataque com uma visualização completa. A análise de segurança de detecção e resposta estendida (XDR) examina um grande volume de informações para identificar uma série de atividades suspeitas. De acordo com a empresa de análise Gartner, o XDR é “uma ferramenta de detecção de ameaças de segurança e resposta a incidentes baseada em SaaS, específica do fornecedor, que integra nativamente vários produtos de segurança em um sistema de operações de segurança coeso”.

A definição de XDR da Forrester Research é um pouco mais ampla: “A evolução do EDR, que otimiza a detecção, investigação, resposta e busca de ameaças em tempo real. O XDR unifica detecções de *endpoint* relevantes para a segurança com telemetria de ferramentas de segurança e negócios, como análise e visibilidade de rede (NAV), segurança de e-mail, gerenciamento de identidade e acesso, segurança na nuvem e muito mais. É uma plataforma nativa da nuvem construída em infraestrutura de big data para fornecer às equipes de segurança flexibilidade, escalabilidade e oportunidades de automação.” A versão destinada à área comercial é licenciada na forma de subscrição por dispositivo.

Entendemos que este cenário apresenta as seguintes vantagens:

- Coleta e correlaciona dados de várias fontes, incluindo *endpoints*, rede, nuvem e outros dispositivos, oferecendo uma visibilidade abrangente das ameaças;
- Identifica padrões de comportamento e correlaciona esses dados para uma resposta assertiva a ataques e vazamento de dados.
- Maior capacidade de detecção de ataque e ameaças;
- Resposta a ameaças de forma automatizada e orquestrada;
- Identifica ameaças ocultas, furtivas e sofisticadas de forma proativa e rápida;
- Rastreia ameaças em qualquer fonte ou local dentro da organização;
- Bloqueia ataques conhecidos e desconhecidos com proteção de *endpoint*;
- Evite a fadiga de alertas;
- Maior velocidade na resposta a ataques; e
- Maior velocidade na contenção a ataques.

Entendemos que este cenário apresenta as seguintes desvantagens:

- Requer maior grau de maturidade das equipes de segurança.
- Potencialmente com maior custo frente a solução do tipo EDR;
- Necessidade de hardware robusto para suportar as atividades de monitoramento contínuo, coleta e análise de dados;
- Potencial restrição de competitividade devido à incipiência dessa solução no mundo tecnológico; e
- Necessidade de corpo técnico dedicado e capacitado para análise e interpretação dos dados de segurança coletados.

A solução de solução de segurança do tipo detecção e resposta estendida se relaciona como uma abordagem holística para a detecção e resposta a ameaças, que envolve a integração e correlação de dados de várias fontes em uma única plataforma. Essa abordagem permite que as equipes de segurança monitorem e analisem as atividades de segurança em toda a infraestrutura de TI, incluindo redes, *endpoints* e aplicativos. Dessa maneira uma solução de segurança avançada integrada de prevenção, detecção e resposta deve ser capaz de analisar os dados coletados em tempo real, utilizando algoritmos avançados para identificar comportamentos suspeitos, devendo ser capaz de compartilhar inteligência de ameaças com outras ferramentas de segurança, como soluções de SIEM/SOAR.

Além disso, essa deverá ser capaz de automatizar a detecção e a resposta a incidentes, incluindo a remediação de ameaças, a isolação de sistemas comprometidos e a coleta de evidências forenses. Isso tudo sem esquecer que ela deverá dispor de uma oferta de relatórios detalhados e trilhas de auditoria para fins de conformidade e gerenciamento de riscos.

Diante disso, em razão dos fatos relatados, a presente solução **demonstra ser tecnicamente viável**.

11. REGISTRO DAS SOLUÇÕES INVIÁVEIS

Conforme § 1º do art. 11 da SGD/ME n.º 94/2022, as soluções detalhadas na tabela a seguir foram consideradas inviáveis, devido às restrições técnicas, legais, econômicas e ausência completa de parâmetros confiáveis de custos para comparação e composição da estimativa de custos (TCO), portanto, dispensamos a realização dos respectivos cálculos do custo total de propriedade para esse item.

Tabela 4 - Registro das soluções inviáveis.

Id.	Descrição da Solução
1	Solução de segurança do tipo antivírus livre ou gratuito.
2	Solução de segurança do tipo antivírus licenciado.

12. ANÁLISE COMPARATIVA DE CUSTOS

A análise comparativa de custos foi elaborada considerando apenas as soluções técnica e funcionalmente viáveis, nos termos do inciso III, do art. 11, da IN SGD/ME n.º 94/2022, e inclui:

a) cálculo dos custos totais de propriedade (*Total Cost Ownership* - TCO) por meio da obtenção dos custos inerentes ao ciclo de vida dos bens e serviços de cada solução, a exemplo dos valores de aquisição dos ativos, insumos, garantia técnica estendida, manutenção, migração e treinamento; e

b) memória de cálculo que referencie os preços e os custos utilizados na análise, com vistas a permitir a verificação da origem dos dados.

12.1. Comparação de custos totais de propriedade

A presente seção descreve de forma comparativa e sintética os custos totais de propriedade projetados para o período de 3 (três) anos, com vistas a apresentar uma melhor visualização do impacto da adoção de cada uma das soluções consideradas viáveis.

Tabela 5 - Comparação de custos totais de propriedade.

Id.	Descrição da Solução	TCO GLOBAL
3	Solução de segurança do tipo detecção e resposta.	R$ 2.555.436,00
4	Solução de segurança do tipo detecção e resposta estendida.	R$ 8.229.781,00

Pode-se observar na tabela acima, que a contratação da solução de segurança do tipo detecção e resposta, apresenta o potencial de economia de **aproximadamente 69% (sessenta e nove) por cento**, frente a contratação da solução de segurança do tipo detecção e resposta estendida.

Consideramos importante registrar que se trata de soluções distintas e que dada imaturidade institucional e ausência de ferramentas básicas de segurança não conseguimos justificar os benefícios de uma solução com essas funcionalidades, razão pela qual, essa análise pode ser feita em momento futuro, a partir do amadurecimento institucional e implementação de ferramentas básicas para sustentar a operação do órgão.

12.2. Memória de cálculo das soluções viáveis

12.2.1. Solução 3: Solução de segurança do tipo detecção e resposta.

Para viabilizar o cálculo comparativo de custos totais de propriedade utilizamos como referência valores praticados em contratos similares, de outros órgãos da Administração Pública Federal, obtidos através de pesquisa textual, no sítio de compras governamentais comprasnet, utilizando como parâmetro de pesquisa os termos **"EDR"**, **"detecção e resposta de *endpoint*"**, **"*endpoint detection and response*" e "proteção de *endpoint*"**, identificamos e selecionamos, em 27/10/2023, 8 (oito) contratações públicas, as quais encontram-se detalhadas no Apêndice II - Análise de Projetos Similares, que apresentam similaridade com esta solução.

Por se tratar de licença de uso de *software*, na modalidade serviço, cuja remuneração ocorre de forma periódica, foi estimado o custo total de propriedade considerando um cenário de utilização contínua, desconsiderando eventuais reajustes e/ou alterações no modelo de negócio e precificação, pelo período de 3 (três) anos.

Para efeitos de composição do custo total de propriedade utilizamos os dados obtidos mediante pesquisa de preços, a qual irá compor a presente instrução processual. Assim sendo, temos o seguinte a seguinte estimativa:

Tabela 6 - Memória de cálculo - Solução de segurança do tipo detecção e resposta.

Id.	Descrição	CATSER	Unidade de medida	Modelo de remuneração	Quantidade	Valor unitário	Valor ano 1	Valor ano 2	Valor ano 3	TCO estimado
1	Solução de segurança do tipo detecção e resposta.	27502	Licença de uso	Parcela anual	16.381	R$ 52,00	R$ 851.812,00	R$ 851.812,00	R$ 851.812,00	R$ 2.555.436,00
Valor Total Estimado							R$ 851.812,00	R$ 851.812,00	R$ 851.812,00	R$ 2.555.436,00

Importante destacar que os códigos CATSER são utilizados de forma genérica, não sendo, portanto, possível concluir que esses dados representam a totalidade das contratações públicas, para esses bens, ocorridas no período, tampouco que esses bens licitados atendem na íntegra a necessidade tratada neste documento.

Além disso, deve-se considerar que os valores refletem exclusivamente as condições conhecidas em contratos e editais, não sendo possível afirmar que tanto os equipamentos descritos sejam plenamente compatíveis com os descritos como necessidade para a contratação. Assim como não é possível compreender, através da pesquisa de preços, o cenário interno e as necessidades específicas de cada órgão contratante.

Portanto, considerando que as diversas soluções podem variar em termos de especificações, os valores devem ser entendidos como simples estimativas utilizadas para a construção de cenários hipotéticos.

12.2.2. Solução 4: Solução de segurança do tipo detecção e resposta estendida.

Para viabilizar o cálculo comparativo de custos totais de propriedade utilizamos como referência valores praticados em contratos similares, de outros órgãos da Administração Pública Federal, obtidos através de pesquisa textual, no sítio de compras governamentais comprasnet, utilizando como parâmetro de pesquisa os termos **"XDR"**, **"detecção e resposta estendida"** e **"*extended detection and response*"**, identificamos apenas 1 (uma) contratação pública, a qual encontra-se detalhada no Apêndice II - Análise de Projetos Similares, que apresentam similaridade com esta solução, bem como suas respectivas atas encontra-se vigentes em 27/10/2023.

Por se tratar de licença de uso de *software*, na modalidade serviço, cuja remuneração ocorre de forma periódica, foi estimado o custo total de propriedade considerando um cenário de utilização contínua, desconsiderando eventuais reajustes e/ou alterações no modelo de negócio e precificação, pelo período de 3 (três) anos.

Para efeitos de composição do custo total de propriedade utilizamos para todos os efeitos os dados do Pregão Eletrônico n.º 11/2023, UASG 254420, de autoria do FUNDAÇÃO OSWALDO CRUZ (FIOCRUZ), datado de 24 de maio de 2023, em cópia no documento id. (125717791), o qual, no entender desta Equipe de Planejamento da Contratação, apresenta melhor correlação com esta solução. Assim sendo, temos o seguinte a seguinte estimativa:

Tabela 6 - Memória de cálculo - Solução de segurança do tipo detecção e resposta estendida.

Id.	Descrição	CATSER	Unidade de medida	Modelo de remuneração	Quantidade	Valor unitário anual	Valor ano 1	Valor ano 2	Valor ano 3	TCO estimado
1	Solução de segurança do tipo detecção e resposta estendida.	27502	Licença de uso	Parcela anual	16.381	R$ 167,00	R$ 2.735.627,00	R$ 2.735.627,00	R$ 2.735.627,00	R$ 8.206.881,00
Valor Total Estimado							R$ 2.735.627,00	R$ 2.735.627,00	R$ 2.735.627,00	R$ 8.206.881,00

Importante destacar que os códigos CATSER são utilizados de forma genérica, não sendo, portanto, possível concluir que esses dados representam a totalidade das contratações públicas, para esses bens, ocorridas no período, tampouco que esses bens licitados atendem na íntegra a necessidade tratada neste documento.

Além disso, deve-se considerar que os valores refletem exclusivamente as condições conhecidas em contratos e editais, não sendo possível afirmar que tanto os equipamentos descritos sejam plenamente compatíveis com os descritos como necessidade para a contratação. Assim como não é possível compreender, através da pesquisa de preços, o cenário interno e as necessidades específicas de cada órgão contratante.

Portanto, considerando que as diversas soluções podem variar em termos de especificações, os valores devem ser entendidos como simples estimativas utilizadas para a construção de cenários hipotéticos.

13. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

Após análise comparativa das soluções viáveis, considerando seus aspectos técnicos e econômicos, esta Equipe de Planejamento da Contratação recomenda o Registro de Preços para eventual **CONTRATAÇÃO DE SOLUÇÃO DE SEGURANÇA DE *ENDPOINT* COM DETECÇÃO E RESPOSTA A AMEAÇAS E INCIDENTES**, **NA MODALIDADE SUBSCRIÇÃO, INCLUINDO SUPORTE TÉCNICO, GARANTIA TÉCNICA, ATUALIZAÇÃO CONTÍNUA, INSTALAÇÃO, CONFIGURAÇÃO E TREINAMENTO,** de acordo com especificações comuns de mercado capazes de atender aos requisitos de negócio.

Tabela 7 - Descrição da solução de TIC a ser contratada.

Item	Descrição da Solução	CATSER	Unidade de medida	Quantidade
1	Solução de segurança do tipo detecção e resposta a ameaças e incidentes, na modalidade subscrição, incluindo suporte técnico, garantia técnica, atualização contínua, instalação, configuração e treinamento.	27502	Licença de uso	16.381

13.1. Detalhamento da Solução de Tecnologia da Informação e Comunicação

A solução de tecnologia da informação ora pretendida é composta pela solução de segurança do tipo detecção e resposta a ameaças e incidentes, incluindo suporte técnico, garantia técnica, atualização contínua, instalação, configuração e treinamento, de acordo com especificações comuns de mercado capazes de atender aos requisitos de negócio, conforme detalhamento a seguir:

13.1.1. Solução de segurança do tipo detecção e resposta a ameaças e incidentes

A solução deverá detectar e bloquear em tempo real ameaças conhecidas e desconhecidas (*zero-day*), ataques *file-less*, ameaças persistentes avançadas (APTs), *ransomwares*, *exploits* e outros comportamentos maliciosos, sem depender exclusivamente de base de assinaturas ou heurísticas;

A solução deverá possuir a capacidade de implementar a funcionalidade de "M*achine Learnin*g" utilizando como fonte de aprendizado a rede de inteligência do fabricante, correlacionando técnicas de proteção com os vetores de ataques, identificando não somente os aspectos maliciosos;

A solução deverá possuir funcionalidades específicas para prevenção contra a ação de *ransomwares* com capacidade, em caso de incidente de restauração dos arquivos comprometidos;

A solução deverá possuir funcionalidade específica de impedir as técnicas de manipulação e randomização de memória impossibilitando a exploração de vulnerabilidades em aplicações;

A solução deverá impedir os ataques direcionados mesmo que utilizando as vulnerabilidades de *zero-day*, mitigando os comportamentos de exploração de vulnerabilidades em aplicações conhecidas, tais como:

- Structured Exception Handler Overwrite Protection (SEHOP);
- Heap Spray (Exploits que iniciam através do HEAP);
- Java Exploit Protection;

A solução deverá efetuar análise baseada em técnicas de *machine learning*, inteligência artificial e *threat intelligence*, permitindo a proteção contra-ataques que explorem vulnerabilidades, mesmo que ainda não existam patches de correção;

A solução deverá realizar análise de comportamento com base nas táticas, técnicas e procedimentos (TTPs) listados no framework MITREATT&CK;

A solução deverá realizar análise dos artefatos em pré-execução, ou seja, antes de serem executados no sistema operacional, evitando que a máquina seja infectada;

A solução deverá detectar e bloquear ameaças que utilizem técnicas de ofuscação e sequestro de *Dynamic-link library* (DLL);

A solução deverá detectar e bloquear técnicas de evasão, incluindo pro*cess injec*tion e uso de executáveis legítimos do *Windows* para rodar scripts e ações maliciosas;

A solução deverá reconhecer padrões e bloquear comportamentos potencialmente maliciosos ou possuir mecanismos automáticos preventivos ou corretivos que sejam capazes de inibir as ações maliciosas resultantes de, no mínimo, 5 (cinco) das ações listadas abaixo:

- Rodar a partir diretórios incomuns (ex: diretório de dados, temp e lixeira);
- Executar elevação de privilégio inesperadas;
- Tentar se passar por processos do Windows;
- Estabelecer conexões de rede suspeitas (*call back ou command & control*);

- Uso suspeito do PSEXEC;
- Invocação maliciosa através do *Rundll*;
- Exploração ou modificação do arquivo *hosts*;
- Tentativa de invocação de Remote Shell.

A solução deverá identificar e bloquear alterações suspeitas em chaves de registro e tarefas agendadas na máquina;

A solução deverá proteger contra macros maliciosas, bem como scripts e comandos *Powershell* maliciosos;

A solução deverá bloquear *exploits* e *payloads* suspeitos do *Metasploit;*

A solução poderá complementar as análises utilizando recursos em nuvem da solução, desde que não incida custos adicionais. Neste caso, será permitido apenas o envio de metadados dos artefatos sob análise, sem submissão do artefato em si ou seu conteúdo à nuvem;

A solução deverá possuir funcionalidade de *Endpoint detection and response* (EDR) e análise forense, provendo uma visão completa do fluxo do ataque e informações detalhadas sobre os comportamentos detectados, de forma a auxiliar e agilizar as ações de remediação;

A solução deverá correlacionar os eventos de detecção e bloqueio de malwares, permitindo sua visualização na console;

A solução deverá permitir configurar regras de exclusão (*whitelists*) de determinados arquivos, diretórios, processos ou aplicativos que não devem ser analisados pela solução;

A solução deverá ser capaz de remover e/ou inativar de forma ágil e eficaz outras soluções de antivírus instaladas nos equipamentos da CONTRATANTE;

A solução deverá coletar as atividades de todos os artefatos analisados, contendo informações sobre interação com outros processos, arquivos e chaves de registro acessadas/modificadas, conexões de rede realizadas, dentre outras;

A solução deverá ter a capacidade de implementar, no mínimo, as seguintes funcionalidades:

- Reputação de arquivos (com ou sem acesso à internet no *endpoint*);
- IPS de Próxima Geração;
- Proteção de navegadores;
- Aprendizado de máquinas;
- Análise comportamental;
- Mitigação da exploração de memória;
- Controle e isolamento de determinadas aplicações;
- Controle de dispositivos;
- Emulação para malware; e
- Proteção ao ambiente de *Active Directory*.

A solução poderá distribuir iscas no ambiente com o objetivo de detectar e interromper tentativas de infiltração, através da implementação de pelo menos:

- Criação de entradas falsas de cache, como Cache de DNS a fim de enganar um invasor e identificar ações maliciosas no ambiente;
- Deve possibilitar a criação de arquivos falsos nas máquinas dos usuários;
- Deve possibilitar a criação e distribuição de senhas falsas nos sistemas a fim de identificar invasores no ambiente;
- Criação de compartilhamentos de rede falsos em desktops;
- Deve ser capaz de enviar alertas quando as “Iscas” falsas são acionadas e/ou modificadas; e
- Deve ter a capacidade de revelar tentativas de ataques dentro da rede interna.

A solução poderá ter a capacidade de bloquear exploits que trabalham em nível de “shell code”;

A solução poderá ter proteção contra técnicas de reconhecimento do domínio, sendo capaz de detectar um invasor que utilize técnicas de movimentação lateral ou roubo de credenciais válidas;

A solução poderá proteger contra intrusões por processo, usuário e terminal;

A solução poderá ser capaz de identificar vulnerabilidades, erros de configurações e possíveis *Backdoors* presentes nos hosts, em especial quando encontradas no *Active Directory*;

A solução poderá ser capaz de proteger alterações no *Active Directory* sem a necessidade de instalação de agentes ou componentes adicionais nas estações de trabalho;

A solução poder ser capaz de detectar e proteger roubos de credenciais no ambiente que utilizem a técnica Pass-the-Hash e Pass-the-Ticket;

Toda a comunicação da solução ser realizada de forma criptografada por meio de protocolo padrão TLS (Transport Layer Security) ou superior;

A solução deverá rastrear arquivos compactados para, no mínimo, os seguintes formatos: ZIP, RAR, TAR, BZ2;

A solução deverá gerar backup de arquivos antes de iniciar o processo de remoção de vírus;

A solução deverá permitir criar regras de firewall de bloqueio/permissão utilizando protocolos TCP/IP e de acordo com as aplicações instaladas nos clientes; e

A solução deverá permitir configuração de HIPS (Host Intrusion Prevention System).

13.1.2. **Console de gerenciamento**

A solução deverá possuir console de gerenciamento central, via protocolo web seguro hospedada no ambiente do próprio fabricante, como serviço SaaS *(Software as a Service),* sem custos adicionais a CONTRATANTE. O console web deve ser acessível por meio de navegadores de Internet, tais como: Google Chrome, versão 100 ou superior, Mozilla Firefox, versão 100 ou superior, e Microsoft Edge, versão 41 ou superior;

A solução deverá possuir acesso precedido de login e senha;

A solução deverá possuir gestão de nível de acesso, para que múltiplos administradores tenham acesso às funcionalidades do sistema de acordo com seu nível de permissão;

A solução deve permitir uma administração por grupos, categorias, características e hierarquizada;

A solução deve permitir o agrupamento dinâmico, ou seja, a criação de grupos que tenham seus membros atualizados automaticamente, baseado em, pelo menos um dos seguintes critérios:

- Endereço IP ou subnet; e
- Etiqueta personalizada (TAG).

A solução deve permitir que políticas criadas por um administrador sejam replicadas aos níveis abaixo na hierarquia;

A solução deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;

A solução deve permitir a criação de regras de liberação e bloqueio para fins de controle de utilização de mídias removíveis em um dispositivo, permitindo especificar número de série, fabricante ou usuário;

A solução deverá possuir todas as funcionalidades requeridas devem fazer parte de um único produto;

A solução deverá permitir até 10 (dez) sessões simultâneas;

A solução deverá permitir aos administradores criarem diferentes políticas de segurança e aplicá-las a diferentes grupos de máquinas de acordo com seus atributos;

A solução deverá manter registro em log de todas as ações de detecção e bloqueio de malware e comportamento malicioso;

A solução deverá funcionalidade de envio logs gerados para um centralizador de eventos, SIEM (system information event manager), ou SOAR (Security Orchestration Automation and Response) ou outro, utilizando protocolo de comunicação como *SYSLOG, CEF, JSON, XML e CSV;*

A solução deverá suportar busca no log pelo IP de Origem, IP de destino, nome da máquina, nome do processo, arquivo e chave de registro;

A solução deverá ser capaz de detalhar as consultas realizadas a fim de avaliação pormenorizadas das ocorrências;

A solução deverá ser possível tomar ações como "quarentenar" a máquina, adicionar o artefato a *blacklist* ou lista de exclusão (*whitelist*), dentre outras;

A solução deverá permitir a geração de relatórios, consulta em log ou dashboard para visualizar, no mínimo, as seguintes informações:

- Eventos de ameaças;
- Eventos de comportamentos suspeitos;
- Malwares detectados e bloqueados;
- Computadores infectados.

A solução deverá possuir a funcionalidade de emissão e o envio de alertas, via e-mail, para usuários pré-cadastrados, em caso de ocorrência de alarmes;

A solução deverá possuir a funcionalidade de emissão e o envio de relatórios periódicos, via e-mail, para usuários pré-cadastrados;

A solução deverá possuir a funcionalidade de exportação de dados nos formatos PDF, HTML e CSV;

A solução deverá manter log de auditoria com registro das configurações realizadas pelos usuários ou administradores da solução;

A solução deverá permitir a visualização do inventário das máquinas que possuem o agente instalado, contendo no mínimo as seguintes informações:

- Nome da máquina;
- Endereço IP;
- Versão do sistema operacional;
- Versão do agente;
- Política aplicada;
- Aplicações instaladas; e
- Serviços com seus respectivos status.

A solução deverá identificar o equipamento que está sofrendo ataques e comandar o agente de *endpoint* para que aquele determinado equipamento seja movido para uma área de quarentena;

A solução deverá suportar que ações de gerenciamento de eventos/incidentes, na console, sejam realizadas de tanto pelo administrador, quando, preventivamente e de forma automática pela solução; e

A solução deverá dispor linha do tempo gráfica, contendo toda a sequência de eventos que ocorreram durante a execução do malware, sendo possível ainda expandir os detalhes de cada informação.

13.1.2.1. **Agentes da solução**

Os agentes da solução devem ser compatíveis com as versões de sistema operacionais:

Para computadores de usuários finais (estações: desktop, workstation e notebooks):

- Microsoft Windows 7 (32-64bit) ou superior.

Para servidores de rede físicos ou virtuais:

- Microsoft Windows Server 2008 (64bit) ou superior.
- Ser suportado em sistemas operacionais Linux (32-64bit)
- O agente deve suportar sua instalação em Sistemas Operacionais virtualizados em ambiente VMware vSphere.

O agente não deve impactar a performance das estações e servidores, gerando baixo consumo de CPU, memória, disco e rede;

A solução deverá ser possível a instalação silenciosa, sem interação com o usuário e sem necessidade de acesso à Internet;

A solução deverá ser possível a instalação e atualização dos agentes de forma manual ou remota, com suporte à distribuição do agente por ferramentas de terceiros, incluindo o System Center Configuration Manager (SCCM) da Microsoft;

A solução deverá ser possível permitir a desinstalação ou alteração da configuração do agente mediante requisição de senha ou token gerados pela console de gerência;

A solução deverá ser possível impedir alterações na configuração do agente por usuários ou processos não autorizados;

A solução deverá ser possível funcionar com agente único na estação de trabalho e servidores físicos e/ou virtuais a fim de diminuir o impacto ao usuário final;

A solução deverá suportar a instalação do agente on-premise, para equipamentos que não podem se conectar à internet, devido a regras de negócio e/ou restrições impostas pelo próprio equipamento, de modo que tais equipamentos possam ser gerenciados, atualizados e protegidos;

A solução deverá realizar suas análises e bloqueios nas estações mesmo quando estiver sem conectividade com os servidores da solução e sem acesso à Internet;

A solução deverá possuir proteção contra desinstalação e/ou desativação dos seus componentes, serviços e processos de forma não autorizada;

A solução deverá realizar a configuração de proxy no agente ou obter as configurações de proxy definidas no próprio sistema operacional;

A solução deverá exibir ou inibir alertas ao usuário em caso de detecção de alguma ameaça, conforme regras definidas pelo administrador;

A solução deverá implementar as seguintes ações de resposta quando uma ameaça ou comportamento malicioso for detectado:

- Ignorar;
- Registrar em log;
- Alertar;

- Bloquear;
- Remover ou quarentenar;

A solução deverá possuir a capacidade de fazer o isolamento da máquina ou grupo de máquinas, sem precisar de nenhuma integração com outros softwares ou dispositivos de rede para isso, de maneira que ela perca a comunicação com a rede ou se comunique apenas com os servidores da solução ou com servidores e serviços definidos na política de isolamento; e

A solução deverá permitir que o administrador efetue a liberação da máquina do isolamento via console de gerência ou fornecer uma chave para realizar a liberação.

13.1.3. **Serviços de suporte técnico**

Entende-se por suporte técnico, o serviço prestado na forma de serviços continuados presenciais e não presenciais, de segundo e terceiro nível, para realização de correções nas aplicações de *software* que compõe a solução contratada, mediante investigação, depuração e correções de falhas técnicas detectadas ou elaboração de alternativas de contorno aos problemas técnicos reportados.

Ainda, são considerados serviços de suporte técnico:

- Orientações para identificação de causa de falhas nas aplicações de *software* e seus componentes;
- Interpretação da documentação das aplicações de *software* e seus componentes;
- Apoio para execução de procedimentos de atualização para novas versões;
- Apoio para uso, configuração, instalação e otimização das aplicações de *software* e seus componentes;
- Orientação para operacionalização da console de gerenciamento;
- Esclarecimento de dúvidas, de forma a garantir o correto funcionamento e utilização das aplicações de *software*, de acordo com as melhores práticas publicadas pelo fabricante.
- Suporte à instalação das licenças/agentes;

Para operacionalização do serviço de suporte técnico, a CONTRATADA deverá disponibilizar uma Central de Atendimento, por meio de canal telefônico ou por meio de área em website, com atendimento em língua portuguesa, falada e escrita no Brasil, para o registro de solicitações de suporte técnico.

Os serviços de suporte técnico deverão ser prestados, de forma ininterrupta 24x7, vinte e quatro horas por dia, sete dias na semana (inclusive feriados), durante toda a vigência da garantia.

O atendimento poderá ser prestado, inicialmente, remotamente, caso exista a necessidade de intervenção técnica nos equipamentos a CONTRATADA deverá proceder o atendimento presencial, no local indicado na requisição.

A CONTRATADA deverá trabalhar, ininterruptamente, na solução dos problemas até que a solução esteja novamente operando em regime normal de produção.

A CONTRATANTE considerará o problema efetivamente solucionado quando o usuário confirmar o atendimento da demanda. Destaca-se que caso o chamado seja rejeitado, esse será reaberto quantas vezes forem necessárias, até sua completa solução, não cabendo ônus pela reabertura dos chamados.

A CONTRATADA poderá efetuar um número ilimitado de chamados de suporte técnico durante a vigência da garantia.

A CONTRATADA deverá disponibilizar documentação em meio eletrônico, no formato PDF pesquisável, contendo toda a descrição detalhada das requisições de suporte técnico referente ao período mensal de prestação de serviço, em língua portuguesa, escrita e falada no Brasil.

13.1.3.1. **Prazos de atendimento**

Os prazos de atendimento e resolução das solicitações de suporte técnico, serão categorizados, conforme se segue:

Tabela 8 - Prazos de atendimento.

Id.	Severidade	Descrição	Tipo de atendimento	Início de atendimento	Prazo de solução	Horário de atendimento	Meta
1	Crítica	Um ou mais serviços não estão acessíveis ou não podem ser usados. A produção, as operações ou as datas limite para implantação são gravemente afetadas, ou há um grave impacto sobre a produção ou as atividades da instituição. Vários usuários ou serviços são afetados.	Remoto, com exceção das situações em que seja necessária intervenção presencial.	1 hora	4 horas	24 horas x 7 dias por semana, inclusive feriados.	90%
2	Alta	O serviço pode ser usado, mas com limitações. A situação tem impacto operacional moderado e é possível lidar com ela durante o horário comercial. Um único usuário, cliente ou serviço é afetado parcial ou totalmente.	Remoto, com exceção das situações em que seja necessária intervenção presencial.	2 horas	8 horas	24 horas x 7 dias por semana, inclusive feriados.	90%
3	Média	A situação tem impacto operacional mínimo. O problema é importante, mas não tem impacto expressivo na produtividade e no serviço atual do cliente. Um único usuário experimenta interrupção parcial, mas existe uma solução alternativa aceitável.	Remoto, com exceção das situações em que seja necessária intervenção presencial.	4 horas	10 horas	10 horas x 5 dias: das 8h às 18h de segunda à sexta-feira, exceto feriados.	90%
4	Baixa	Chamados associados a pedidos de orientações, apoio, interpretações, suporte à instalação das licenças/agentes, esclarecimentos de dúvidas.	Remoto.	8 horas	16 horas	10 horas x 5 dias: das 8h às 18h de segunda à sexta-feira, exceto feriados.	90%

Início Atendimento: é o tempo entre o registro da solicitação pelo usuário na Central de Atendimento ou por telefone a CONTRATADA, e o primeiro atendimento

da CONTRATADA;

Caso a CONTRATADA receba o chamado por telefone, essa deverá registrar a requisição com, minimamente, nome e telefone de contato do requisitante, problema ou incidente reportado e local de atendimento.

Prazo para Solução: é o tempo entre a registro da solicitação pelo usuário Central de Atendimento, por meio de canal telefônico ou por meio de área em website à CONTRATADA, e a solução do problema pela CONTRATADA;

A contagem do prazo de solução é registrada com a solução da problemática que originou o chamado ou aplicação de contorno, que tornou o serviço novamente operacional;

Os prazos de atendimento e execução são contados em HORAS corridas;

As metas de desempenho servirão para a aferição mensal dos indicadores de medição de resultados exigidos na prestação dos serviços. Para cada uma das metas, há indicadores de glosa por não atingimento das metas definidas;

Os chamados não atendidos dentro das metas de desempenho deverão ser atendidos dentro da meta de desempenho do nível de severidade superior ao de sua classificação inicial;

Após a solução do chamado, a CONTRATANTE terá o prazo de até 90 (noventa) dias corridos para solicitar esclarecimentos atinentes ao chamado e/ou para efetuar testes na solução empregada;

O chamado técnico só será encerrado com a anuência da CONTRATANTE.

a) **Escalação de severidade**

Por necessidade do serviço ou criticidade do problema, a SES-DF poderá realizar a escalação de severidade do chamado para níveis superiores de severidade.

No caso de não cumprimento dos prazos na nova severidade, as penalidades decorrentes serão aplicadas conforme severidade da escalação, considerando o prazo total desde a abertura do chamado original.

13.1.4. **Garantia técnica**

Entende-se por garantia técnica o direito da CONTRATANTE em solicitar a CONTRATADA ações corretivas visando à eliminação de problemas identificados na solução de maneira a retorná-los à sua plena condição de funcionamento e desempenho;

Assim, todos os componentes da solução deverão ser cobertos por garantia durante a vigência do contrato, a contar da data de emissão do Termo de Recebimento Definitivo, e, adicionalmente, durante 3 (três) meses após o encerramento contratual, sem custos adicionais à CONTRATANTE;

Para todos os efeitos, a garantia a ser inicialmente prestada será na modalidade online. No entanto, caso haja necessidade, esta deverá ocorrer na modalidade on-site, ou seja, deverá ser realizada de forma presencial nas dependências dos estabelecimentos de saúde da CONTRATANTE.

A emissão do Termo de Recebimento Definitivo não exime a CONTRATADA da responsabilidade pela correção de erros porventura identificados, desde que o erro ou falha, comprovadamente, não se dê em função de falhas da unidade solicitante dos serviços;

Na incidência de acionamento da garantia, essa se dará por meios dos canais oficiais de comunicação estabelecidos entre as partes, os quais deverão permanecer ativos durante todo o período de garantia;

A não observância do prazo para correção de defeito implica execução das penalidades cabíveis estabelecidas em contrato.

13.1.5. **Atualização contínua**

Entende-se por atualização contínua o fornecimento de novas versões corretivas ou evolutivas das aplicações de *softwares* contratadas e lançadas durante a vigência contratual, mesmo em caso de mudança de designação do nome das aplicações de *softwares. As* atualizações deverão compreender a correção de falhas no produto, independentemente de correções tornadas públicas, desde que tenham sido detectadas e formalmente comunicadas à CONTRATADA.

Caso sejam detectados bugs ou falhas nas aplicações de *software*, a CONTRATADA deverá fornecer atualizações de versão necessárias à correção do problema.

A cada nova liberação de versão, a CONTRATADA deverá fornecer as atualizações de manuais e demais documentos técnicos, bem como nota informativa das novas funcionalidades implementadas nesta nova versão.

As atualizações de versões das aplicações de *software* contratadas deverão ser as mais recentes e disponíveis no mercado pelo fabricante.

As novas versões dos produtos contratados, quando aplicáveis, deverão ser disponibilizadas em até 30 (trinta) dias, a partir do lançamento oficial da nova versão.

Em caso de atualização do produto a CONTRATADA se obriga a enviar notificação formal à CONTRATANTE, bem como o *software* atualizado ou sua atualização propriamente dita em mídia digital (pen drive ou unidade de armazenamento externo) ou *link* e permissão para *download* em ambiente seguro na internet ou nuvem.

Quando das atualizações, a CONTRATADA deverá prestar todo o suporte técnico e orientação à equipe da CONTRATANTE quanto aos procedimentos de atualização das aplicações de *softwares* contratados e respectivas licenças, assim como para a migração das bases de dados, criação de cópia de segurança, procedimento de parada e *restart*, caso necessário.

O idioma das aplicações de *software* deve ser obrigatoriamente a língua portuguesa, falada e escrita no Brasil.

13.1.6. **Serviço de instalação e configuração**

Os serviços de instalação e configuração envolvem todas as atividades necessárias à colocação da solução em pleno funcionamento, atendendo as especificações técnicas e demandas de configuração requeridas pela CONTRATANTE. O escopo desses serviços contempla as seguintes atividades:

- Configuração da console de gerenciamento em ambiente de nuvem;
- Configuração completa da solução, incluindo o apoio na definição de políticas e melhores práticas de segurança;
- Configuração de dashboards, relatórios e alertas, de maneira coordenada com a CONTRATANTE;
- Customização dos pacotes de instalação dos agentes e distribuição a todas as estações da CONTRATANTE;
- Entrega da documentação da solução, relatório das atividades e configurações realizadas; e
- Apresentação da solução configurada e implantada.

13.1.7. **Serviço de treinamento**

A CONTRATADA deverá providenciar treinamento referente às fases de instalação, parametrização, monitoramento, melhores práticas e atuação de incidentes, aos colaboradores e técnicos da CONTRATANTE;

O treinamento deverá compreender todas as informações de configuração, operação e gerência de todos os componentes envolvidos na solução adquirida;

A CONTRATADA deverá providenciar todos os recursos necessários para a realização das atividades, incluindo, material, equipamentos, instrutores certificados e local, exceto, eventuais despesas com transporte, alimentação e hospedagem dos participantes da CONTRATANTE;

O treinamento deverá ser baseado no conteúdo programático dos treinamentos oficiais do fabricante da solução e ministrada por empresa devidamente certificada pelo

fabricante;

A CONTRATADA deverá providenciar o treinamento para até 8 (oito) colaboradores, divididos em 2 (duas) turmas com até 4 (quatro) colaboradores, as quais deverão ser realizadas em até 60 (sessenta) dias corridos, após o acionamento;

O treinamento deverá ser realizado em sessões de, no mínimo, 4 (quatro) horas diárias, com carga horária total de, no mínimo, 20 (vinte) horas;

Este treinamento deverá ocorrer na forma presencial, do tipo *hands on*, em local a ser disponibilizado pela CONTRATADA, na cidade de Brasília/DF;

Não serão aceitos treinamentos de aulas gravadas ou por meio de EAD;

A CONTRATADA deverá disponibilizar, digitalmente, em formato PDF pesquisável, os descritivos dos assuntos ministrados no treinamento, que deverão ser avaliados e aprovados pela CONTRATANTE previamente;

O conteúdo programático deverá abranger, no mínimo, os seguintes tópicos:

- Tecnologias utilizadas na solução descrita nesta especificação;
- Instalação, configuração e operação dos agentes;
- configuração e operação da console de gerenciamento;
- Resolução de problemas;
- Administração e gerenciamento da solução;
- Procedimentos de atualização;
- Criação de grupos e políticas;
- Extração de Relatórios; e
- Consultas.

O cronograma de realização do treinamento será definido em comum acordo, entre a CONTRATADA e CONTRATANTE;

Após a conclusão do treinamento a CONTRATADA deverá realizar uma avaliação de conhecimentos básicos necessários para operação dos equipamentos;

Concluído todo o processo de treinamento, deverá ser fornecido aos participantes, certificado de conclusão, emitido por empresa credenciada pelo fabricante; e

O idioma do material didático fornecido para o treinamento deve ser obrigatoriamente a língua portuguesa, falada e escrita no Brasil.

13.1.8. **Prazos de entrega**

As licenças do software contratadas, bem como suas chaves de ativação, devem ser disponibilizadas em até **15 (quinze) dias corridos** após a emissão da Ordem de Serviço (OS), podendo ser prorrogado por igual período desde que requerido pela CONTRATADA e autorizado pela CONTRATANTE.

A solução deverá estar completamente disponibilizada, instalada, configurada e operacional em até **60 (sessenta) dias corridos**, contados a partir da data de emissão da Ordem de Serviço.

14. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

Com base em pesquisa mercadológica estimamos que o valor global da contratação seja de **R$ 851.812,00 (oitocentos e cinquenta e um mil oitocentos e doze reais) ,** conforme detalhamento na tabela a seguir:

Item	Descrição	CATSER	Unidade de Medida	Quantidade	Valor unitário	Valor total anual
1	Solução de segurança do tipo detecção e resposta a ameaças e incidentes, na modalidade subscrição, incluindo suporte técnico, garantia técnica, atualização contínua, instalação, configuração e treinamento.	27502	Licença de uso	16.381	R$ 52,00	R$ 851.812,00
Valor Total Estimado			**R$ 851.812,00**			

15. JUSTIFICATIVA TÉCNICA DA ESCOLHA DA SOLUÇÃO

Nos últimos anos as entidades governamentais no mundo todo vêm sofrendo diversos ataques no âmbito digital, incluindo ataques de negação de serviço, roubo de informações, alterações de páginas e de dados, ataques direcionados e persistentes. Estes eventos contribuem para um enorme prejuízo em relação às suas imagens públicas, pois tais entidades prestam serviços à sociedade como um todo e mantêm na sua base inúmeros dados pessoais da população.

Para proteção dos dados produzidos e custodiados é necessário que os órgãos públicos invistam cada vez mais em mecanismos de proteção cibernética. Dispositivos finais de usuários em um órgão sempre foram considerados pontos de entrada para pragas digitais e como cada dia mais as organizações têm liberado acesso à Internet por parte de seu corpo funcional, a superfície de contato para execução de tais aplicativos maliciosos é cada vez maior.

Logo, a implementação de uma solução de segurança com detecção e resposta a ameaças e incidentes, para computadores, notebooks e servidores, consiste na proteção básica do parque de ativos computacionais, visando oferecer proteção a todos os serviços e dispositivos finais conectados à rede corporativa.

Em termos de economicidade, sob o aspecto financeiro, a vantajosidade econômica potencial foi evidenciada na análise de Custo Total de Propriedade, a qual revelou, que a contratação de solução de segurança com detecção e resposta a ameaças e incidentes na modalidade licenciamento subscrição, em um horizonte de 5 (cinco) anos, desconsiderando a hipótese de eventual upgrade de versão, menos onerosa frente a contratação em mesma modalidade de licenciamento de objeto similar.

Quanto aos aspectos operacionais, a solução de segurança com detecção e resposta a ameaças e incidentes, para computadores, notebooks e servidores proporcionará o gerenciamento centralizado dando visibilidade ao administrador da solução sobre todos os problemas e ameaças que estão em curso ou foram eliminadas do ambiente computacional do órgão. Ainda, viabilizará a automatização do tratamento e correlação de incidentes de segurança cibernética.

No que se refere aos aspectos tecnológicos, a contratação em tela, com o provimento dos serviços agregados de suporte técnico e garantia de atualização, proporcionarão acesso contínuo às novas versões, releases e patchs de correção, mantendo assim a segurança dos dispositivos finais.

Outrossim, o modelo de contratação proposto se mostra aderente a realidade da CONTRATANTE, que por sua atividade finalística constantemente necessita ampliar a prestação de serviços à Sociedade, seja por meio da abertura de novos estabelecimentos de saúde, seja pela ampliação dos existentes. Sendo assim, há frequente demanda por mais microcomputadores e consequentemente por licenças de software de proteção, os quais são necessárias para estabelecer as condições básicas de operação desses serviços, razão pela qual há sabida necessidade de se manter saldo contratual para o atendimento tempestivo das demandas.

Portanto, a escolha pela contratação na forma delineada neste Estudo esta pautada em critérios econômicos, operacionais e tecnológicos, além de trata-se importante mecanismo para fortalecimento dos controles de segurança no tratamento de incidentes de segurança cibernéticas relacionadas ao vazamento de dados, focada em dispositivos finais.

15.1. **Dos diferentes modelos de prestação do serviço**

De forma geral a licenciamento por subscrição de uso de software é menos onerosa para a Administração do que quando o software é adquirido na modalidade de licenciamento perpétuo. Ainda, analisando as principais diferenças na modalidade de licenciamento, a opção pelo licenciamento perpétuo transforma a Administração em refém do fabricante durante o período contratado e após esse período, visto que ou a Administração adquire o serviço de manutenção e suporte anual para garantir as atualizações e suporte técnico ou deverá manter a solução em uso sem atualização e suporte ou, no limite, optar pelo desuso.

Com essas possibilidades a Administração é compelida a arcar com custos elevados na contratação inicial e depois se vê obrigada a contratar os serviços continuados de suporte técnicos e atualização de versão ou, até mesmo, deixando de utilizar a solução "perdendo" assim os montantes investidos até aquele momento.

Ademais, quando da aquisição de uma solução o prazo de garantia na modalidade de licenciamento perpétuo varia de 12 (doze) a 60 (sessenta) meses. Ao longo desse tempo o mercado pode mudar muito e essa solução não ser mais a ideal em comparação à outras novas que porventura venham a entregar novas funcionalidades ou mudança de abordagem frente às diferentes formas que surgem ao longo do tempo dessa forma o valor investido na compra da solução tende a ser perdido.

Assim, observa-se que de acordo com os pontos levantados a escolha de adquirir as soluções de *software* na modalidade de licenciamento perpétuo apresenta sérios riscos ao negócio, demonstrando ir na contramão dos princípios balizadores das contratações públicas, quais sejam: eficiência, eficácia e economicidade.

Pelo exposto, é conveniente e/ou oportuna o licenciamento na modalidade subscrição por dispositivo, cujo modelo se notabiliza por pagar pelo serviço da licença durante o período que a CONTRATANTE julgar necessário obtendo os benefícios e entregáveis planejados. Caso chegue o momento que determinada solução esteja defasada e/ou não faça mais sentido sua utilização poderá a CONTRATANTE deixar este licenciamento de lado visto que a contratação se dá por um modelo de prestação de serviços.

Além disso, essa estratégia permite que o órgão contratante mantenha seu corpo técnico atualizado, pois a cada nova contratação esse é capacitado para operação e uso da nova solução, a qual encontra-se atualizada em relação a seus concorrentes.

15.2. **Parcelamento ou não parcelamento da solução**

Considerando o disposto no inciso I do §2° do art. 12 da IN SGD/ME n.º 94/2022 a Equipe de Planejamento da Contratação deve avaliar a viabilidade de "realizar o parcelamento da solução de TIC a ser contratada, em tantos itens quanto se comprovarem técnica e economicamente viáveis", com vistas ao melhor aproveitamento dos recursos disponíveis no mercado e à ampliação da competitividade sem perda da economia de escala.

Em linha com essa definição a Súmula TCU nº 247 dispõe que é obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes que, embora não dispondo de capacidade para a execução, fornecimento ou aquisição da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas, devendo as exigências de habilitação adequar-se a essa divisibilidade.

Outrora esse entendimento, consideramos que não é possível afirmar sumariamente, sem a análise do caso concreto, que a licitação por itens ou por lote único seria mais eficiente. O próprio TCU já teve a oportunidade de se manifestar no sentido de que, no caso específico, a licitação por lote único seria a mais eficiente à administração:

> "Cabe considerar, porém, que o modelo para a contratação parcelada adotado nesse parecer utilizou uma excessiva pulverização dos serviços ... Esta exagerada divisão de objeto pode maximizar a influência de fatores que contribuem para tornar mais dispendiosa a contratação (...) embora as estimativas numéricas não mostrem consistência, não há nos autos nenhuma evidência no sentido oposto, de que o parcelamento seria mais vantajoso para a Administração. Ao contrário, os indícios são coincidentes em considerar a licitação global mais econômica" (Acórdão nº 3140/2006 do TCU).

A SES-DF busca sempre manter o máximo alinhamento entre a legislação e os normativos que regulam as contratações públicas de soluções de TIC e o atendimento às necessidades técnicas definidas, visando o correto compromisso entre a viabilidade técnica e econômica dessas contratações.

No caso tratado neste ESTUDO, constatamos que a pretensa contratação limita-se a aquisição de um único item, inexistindo, portanto, o parcelamento da solução.

15.3. **Enquadramento legal e normativo**

Quanto ao tipo bem, em conformidade com o parágrafo único, com o art. 114, do Decreto n.º 44.330 de 16 de março de 2023, que Regulamenta a Lei Federal n.º 14.133, de 1º de abril de 2021, Lei de Licitações e Contratos Administrativos, no âmbito da Administração Pública direta, autárquica e fundacional do Distrito Federal, o objeto deste Estudo Técnico enquadra-se como "BEM E/OU SERVIÇO COMUM" por apresentar, independentemente de sua complexidade, "padrões de desempenho e qualidade objetivamente definidos em edital, por meio de especificações usuais no mercado". Por esse motivo e em não se tratando de aquisição de alto vulto não será realizado o procedimento de audiência e/ou consulta pública, para fins de coleta de contribuições.

Tendo em vista não se tratar de aquisição de alto vulto não será realizado o procedimento de audiência e/ou consulta pública, para fins de coleta de contribuições. No que se refere ao Plano Anual de Compras e Contratações, a pretensa contratação encontra-se devidamente prevista, conforme evidencia-se no processo SEI 00060-00225508/2022-19.

15.4. **Alternativa para o modelo de contratação**

Quanto à adoção do Sistema de Registro de Preços (SRP), a Lei Federal n.º 14.133, de 1º de abril de 2021, em seu art. 82, estabelece que "processamento por meio de sistema de registro de preços, à luz do princípio da eficiência, o SRP tem por escopo instrumentalizar meios para aquisição parcelada de bens e serviços pela Administração Pública, sendo, portanto, compatível com a modalidade Pregão Eletrônico (Lei n.º 10.520, de 17 de julho de 2002, art. 11). Ainda, de acordo com o disposto no incisos I a IV, do art. 190, do Decreto n.º 44.330, de 16 de março de 2023, a utilização do Sistema de Ata de Registro de Preços enquadra-se nas seguintes hipóteses:

> (...)
>
> Art. 190. O Sistema de Registro de Preços será adotado, preferencialmente:
>
> I - quando, pelas características do bem ou serviço, houver necessidade de contratações frequentes;
>
> II - quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou tarefa;
>
> III - quando for conveniente a aquisição de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, ou a programas de governo; ou
>
> IV - quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.
>
> (...)

Por outro lado, de acordo com o art. 83 do Lei Federal n.º 14.133, de 1º de abril de 2021, preconiza que "A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente motivada."

Essa estratégia é mais largamente aplicável e recomendável quando se envolve a aquisição com variação temporal, ou seja, soluções cuja demanda pode ser realizada em momentos temporais distintos. Entendemos que esse é o caso da aquisição ora pretendida neste instrumento de planejamento, visto que a solução foi desenhada tecnicamente considerando as necessidades específicas desta Secretaria. Assim, recomendamos que seja utilizado o **Sistema de Ata de Registro de Preços.**

15.5. **Contratações correlatas e/ou interdependentes**

Não foram identificadas contratações correlatas. Quanto a contratações interdependente, todos os objetos necessários ao completo funcionamento da solução de TIC, foram inventariados, quantificados e estão abarcados na contratação ora pretendida.

15.6. **Alinhamento estratégico**

O alinhamento estratégico entre a área de Tecnologia da Informação e a área de negócios da SES-DF, vem sendo requerido pela sua Direção, com o objetivo de atender à demanda por alta qualidade em seus serviços, economia, confiabilidade, flexibilidade, agilidade e racionalização de seus fluxos de trabalho.

Nesse contexto, o Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC 2024-2025 reflete o amadurecimento do nível de governança em Tecnologia da Informação e Comunicações (TIC), do órgão, fruto da atuação do Comitê Gestor de Informática e Informação - CGII e do empenho e árduo trabalho dos servidores deste órgão, que com afinco e competência participaram da elaboração desta importante ferramenta para o alcance de sua missão institucional.

Buscando um alinhamento com as demais áreas e objetivando alcançar melhores resultados, bem como considerando a alta dependência da Organização sobre a sua infraestrutura tecnológica, sistemas de informação e serviços de TI, cuja interrupção no fornecimento dos serviços providos pela área de TI aos seus usuários, impediriam que o Órgão prestasse os serviços públicos que lhe são atribuídos no âmbito do Distrito Federal, foi definido no PDTIC 2024-2025, ações estratégicas visando seu alcance, conforme descrito abaixo:

Tabela 10 - Alinhamento aos planos estratégicos.

Id.	Objetivos Estratégicos
OETIC5	Implementar mecanismos de segurança da informação em 100% do parque computacional

Tabela 11 - Alinhamento com o PDTIC.

Id.	Ação	Id.	Meta
A45	Contratação de solução de Segurança da Informação e Comunicação.	M5.3	Implementar mecanismos de segurança da informação em 100% do parque computacional.

No que se refere ao Plano Anual de Compras e Contratações, o objeto da pretensa contratação encontra-se devidamente prevista, conforme evidencia-se no portal de compras do Governo do Distrito Federal, disponível em: https://portal.compras.df.gov.br/, conforme detalhado na tabela a seguir:

Tabela 12 - Alinhamento com o PAC.

Id.	Descrição
21722	Aluguel de softwares ou licenciados prontos (Software de Prateleira) Serviço de subscrição de Solução de Segurança de EndPoint com detecção e resposta a ameaças e incidentes, incluindo serviços continuados de suporte técnico, garantia técnica, atualização de versões e o provimento de serviços agregados de instalação, configuração e treinamento.

16. JUSTIFICATIVA ECONÔMICA DA ESCOLHA DA SOLUÇÃO

Conforme demostrado na análise comparativa de custo, a contratação da solução de segurança do tipo detecção e resposta a ameaças e incidentes, incluindo serviços de suporte técnico, garantia técnica, atualização contínua, instalação, configuração e treinamento representa uma economia de **aproximadamente 69% (setenta e nove) por cento**, frente a contratação da solução segurança do tipo detecção e resposta estendida, ambas na modalidade subscrição.

17. BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

Os benefícios a serem alcançados com a presente contratação, em termos de eficácia, eficiência, efetividade e economicidade, são:

a) Assegurar a confiabilidade, disponibilidade e integridade dos dados e das informações do órgão, ou àquelas sob sua custódia;

b) Manter a disponibilidade na prestação de serviços, com a promoção de recursos suficientes e adequados às atividades do órgão;

c) Manter atualizados os recursos de segurança da informação do órgão, de forma a prover com rapidez, eficiência e eficácia plena capacidade de atender e suportar as necessidades de negócio;

d) Mitigar possíveis riscos, ameaças, danos ou indisponibilidade aos seus ativos de TI; e

e) Prover monitoramento a eventos de segurança da informação ocorridos no ambiente de TI.

18. PROVIDÊNCIAS A SEREM ADOTADAS

A área requisitante deverá realizar contínuo monitoramento da execução contratual, com o objetivo de garantir a continuidade dos serviços e evitar sua interrupção de forma não programada. Além disso, deverá atuar no sentido de manter sob seu controle o conhecimento do serviço e dos processos de execução de modo a reduzir o risco de dependência em relação ao fornecedor. Todos os eventos da execução contratual deverão ser apontados em registro histórico adequado. Os RISCOS mapeados estão listados no documento MAPA DE RISCOS.

19. POSSÍVEIS IMPACTOS AMBIENTAIS

Não foram identificados impactos ambientais decorrentes da contratação que se pretende levar a efeito.

20. ESTRATÉGIA DE CONTINUIDADE

Por se tratar de aquisição, via Registro de Preços, recomendamos que a vigência do CONTRATO seja fixada em **12 (doze) meses,** contados a partir da data de sua assinatura, podendo ser prorrogado por iguais e sucessíveis períodos até o limite de 120 (cento e vinte) meses, conforme disciplinado no arts. arts. 106 e 107 da Lei Federal n. º 14.133, de 1º de abril de 2021.

Com relação à manutenção das condições iniciais de habilitação técnica, a equipe de fiscalização deve atentar-se ao cumprimento do disposto na letra I, do inciso II, do art. 33, da IN SGD/ME n.º 94/2022:

> (...)
> Art. 33 O monitoramento da execução deverá observar o disposto no Modelo de Gestão do Contrato, e consiste em:
> (...)
> II - a cargo do Fiscal Técnico do Contrato:
> (...)

l) verificar a manutenção das condições classificatórias referentes à pontuação obtida e à habilitação técnica, em conjunto com o Fiscal Administrativo do Contrato;

(...)

A área requisitante deverá realizar contínuo monitoramento da execução contratual, com o objetivo de garantir a continuidade dos serviços e evitar sua interrupção de forma não programada. Além disso, deverá atuar no sentido de manter sob seu controle o conhecimento do serviço e dos processos de execução de modo a reduzir o risco de dependência em relação ao fornecedor. Todos os eventos da execução contratual deverão ser apontados em registro histórico adequado. Os RISCOS mapeados estão listados no documento MAPA DE RISCOS.

21. RECURSOS NECESSÁRIOS

Para viabilizar à implantação e à manutenção da solução identificamos a necessidade dos seguintes recursos:

21.1. Recursos Humanos

Para cumprir as atividades de gestão e fiscalização do CONTRATADA a CONTRATANTE deverá dispor de servidores (titulares e substitutos) para executar os seguintes papéis:

a) Gestor do Contrato: servidor com atribuições gerenciais, designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente;

b) Fiscal Técnico: servidor representante da Área de Tecnologia da Informação, indicado pela autoridade competente dessa área para fiscalizar tecnicamente o contrato;

c) Fiscal Requisitante: servidor representante da Área Requisitante da Solução, indicado pela autoridade competente dessa área para fiscalizar o contrato do ponto de vista funcional da Solução de Tecnologia da Informação; e

d) Fiscal Administrativo: servidor representante da Área Administrativa, indicado pela autoridade competente dessa área para fiscalizar o contrato quanto aos aspectos administrativos.

Destacamos que atualmente a Gerência de Atendimento (GEAT) conta com um quadro total de 8 (oito) servidores. Nesse cenário, se considerarmos a necessidade de indicação de fiscais requisitantes e técnicos, ambos advindos dessa Gerência (incluindo titulares e substitutos), seriam necessários 4 (quatro) servidores, portanto, 50% da força de trabalho dessa área. Logo, mesmo considerando a coexistência de outros contratos, embora isso represente uma importante carga de trabalho, a área dispõe de servidores em quantidade e capacidade minimamente suficientes para a fiscalização de todos os controles, acompanhamento processual e demais atividades necessárias à aferição das exigências contratuais.

22. DECLARAÇÃO DE VIABILIDADE

O presente ESTUDO TÉCNICO PRELIMINAR, elaborado pelos integrantes TÉCNICO e REQUISITANTE em harmonia com o disposto no § 1º do art. 11 da IN SGD/ME n.º 94/2022, considerando a análise das alternativas de atendimento das necessidades elencadas pela área requisitante e os demais aspectos normativos, conclui pela VIABILIDADE da contratação, uma vez considerados os seus potenciais benefícios em termos de eficácia, eficiência, efetividade e economicidade. Em complemento, os requisitos listados atendem adequadamente às demandas formuladas, os custos previstos são compatíveis e os riscos identificados são administráveis, pelo que RECOMENDAMOS o prosseguimento da pretensão.

23. RESPONSÁVEIS

Nos termos do §2° do art. 11 da IN SGD/ME n.º 94/2022, o presente Estudo Técnico Preliminar é aprovado e assinado pelos Integrantes Técnico e Requisitante da Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC.

FÁBIO AYUB BRASIL

Integrante Requisitante

OSMAR DA SILVA FERREIRA

Integrante Técnico

ANDERSON JESUS DE MENEZES

Autoridade de TIC

Apêndice I - Mapa Comparativo das Soluções

Tabela 1 - Apêndice I - Mapa comparativo das soluções.

Requisito	Solução 1	Solução 2	Solução 3	Solução 4
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Não localizada	Sim	Sim	Sim
A Solução está disponível no Portal do *Software* Público Brasileiro, nos termos da Portaria STI/MP nº 46, de 28 de setembro de 2016, e suas atualizações?	Não	Não	Não	Não
A Solução é um *software* livre ou *software* público?	Sim	Não	Não	Não
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	Sim	Sim	Sim	Sim
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Não se aplica	Não se aplica	Não se aplica	Não se aplica
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Não se aplica	Não se aplica	Não se aplica	Não se aplica

Há necessidade de adequação do ambiente?	Não há necessidade	Não há necessidade	Não há necessidade	Não há necessidade
Qual o modelo de contratação?	Não se aplica	Contratação de serviços	Contratação de serviços	Contratação de serviços
Qual a forma de contratação?	Não se aplica	Nova contratação (Licitação)	Nova contratação (Licitação)	Nova contratação (Licitação)

Apêndice II - Lista de Potenciais Fornecedores

Por meio de pesquisa nos participantes dos pregões identificados como projetos similares, constatamos os seguintes potenciais fornecedores:

Tabela 1 - Apêndice II - Lista de potenciais fornecedores.

Fornecedor	CNPJ	Endereço eletrônico	Contato	Correio eletrônico	Telefone
5 Instituto Tecnológico	27.685.014/0001-42	https://www.5it.com.br/	Edmundo Pinheiro	edmundo@5IT.com.br	(61) 98138-8139
Blue Eye Soluções em Tecnologia Ltda	26.025.401/0001-90	https://www.blueeye.com.br/	Rinaldo Araújo	comercial@blueeye.com.br	(61) 98195-0705
Backup Já Segurança Cibernética Ltda	12.818.732/0001-72	https://backupja.com.br/	Philip Obrien	licitacao.obrien@gmail.com	(49) 99132-9784
ISTI Informática e Serviços Ltda	10.554.387/0001-81	https://www.isti.inf.br/	Gustavo de Lena	comercial@isti.inf.br	(61) 98124-0549
Fast Help Informática Ltda	05.889.039/0001-25	https://www.fasthelp.com.br/	Leonardo Vinicius	comercial@fasthelp.com.br	(61) 3363-8636
Future Technologies lnformática Ltda	01.933.257/0001-69	https://www.future.com.br/	André Luis	licitacao@future.com.br	(24) 2232-5850
ISH Tecnologia S/A	01.707.536/0001-04	https://www.ish.com.br/	Vitor Teixeira	licitacoes@ish.com.br	(27) 3334-8900
NetSafe Corp	03.476.184/0002-30	www.netsafecorp.com.br	Waldo Baptista	mario.paini@netsafecorp.com.br	(61) 3030-3333
DFTI - Tecnologia da Informação	09.650.283/0001-91	www.dfti.com.br	Fabrício Bombarda	dfti@dfti.com.br	(61) 3030-1000
Microhard informatica Ltda	42.832.691/0001-30	https://microhard.com.br/	José Glicerio	glicerio@microhard.com.br	(31) 3281-5522
AX4B Sistemas de Informática Ltda	22.233.581/0001-44	https://ax4b.com/	Antônio Cesar	licitacoesbr@ax4b.com	(11) 3230-2760
Alltech Soluções em Tecnologia Ltda	21.547.011/0001-66	https://alltechsolucoes.com.br/	Murilo Rossetto	mrossetto@alltechsolucoes.com.br	(61) 3344-0236
Service IT	12.373.559/0001-46	https://service.com.br/	Laisa Maria	comercialrj@service.com.br	(21) 2246-5815

Apêndice III - Análise de Projetos Similares

A análise comparativa de projetos similares, nos termos da letra a, do inciso II do art. 11 da IN SGD/ME n.º 94/2022, visa analisar as alternativas para atendimento da demanda considerando os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação. Para isso, a partir de busca textual no sítio de compras governamentais comprasnet, identificamos e selecionamos de forma aleatória8 (oito) contratações públicas, que apresentam similaridade com o objeto deste estudo. Os projetos que originarem a contratação desses itens estão detalhamento na tabela a seguir:

Tabela 1 - Apêndice III - Análise de Projetos Similares - Solução de segurança do tipo detecção e resposta.

Pregão	Unidade de Fornecimento	UASG - Unidade Gestora	Data da Compra

114/2023	Objeto: Pregão Eletrônico: Aquisição de licenças de uso de solução corporativa de Segurança de Endpoint's e Servidores para múltiplas plataformas incluindo garantia, suporte e atualização para utilização no parque tecnológico do Governo do Estado de Minas Gerais, sob demanda, futura e eventual.	SEPLAD-MG	01/06/2023
10363/2023	Objeto: Aquisição de solução de segurança de endpoints (antivírus) com licenciamento, instalação e suporte técnico pelo período de 36 (trinta e seis) meses, a serem utilizados nos computadores e servidores das alagoas previdência.	925998	04/08/2023
11/2023	Objeto: Pregão Eletrônico: Contratação de uma solução de proteção contra ameaças avançadas (Next Generation Antivírus - NGAV) baseada em agente com funcionalidade de EDR ("Endpoint Detection and Response"), com suporte, garantia e atualização por 36 meses, conforme condições, quantidades e exigências estabelecidas no Edital e seus anexos.	193099	22/08/2023
24/2023	Objeto: Pregão Eletrônico: Registro de preços para eventual aquisição de licenças, subscrições, softwares e certificado digital, conforme condições, quantidades e exigências do Edital e seus anexos	153030	31/08/2023
3/2023	Objeto: Pregão Eletrônico: Aquisição de equipamentos e materiais de tecnologia da informação e licenças de antivírus, visando atualizar e renovar o parque tecnológico de equipamentos e software do Regional, de acordo com as quantidades e especificações técnicas constantes no Termo de Referência Anexo I do Edital.	389086	10/07/2023
90001/2024	Objeto: Pregão Eletrônico: Registro de preços para a eventual aquisição e renovação de licenças Kaspersky Endpoint Security for Business Select Brazilian Edition com upgrade para ADVANCED, para fins de proteção da rede lógica, equipamentos de TI e informações, por um período de atualização, suporte e assistência técnica de 36 (trinta e seis) meses	925129	11/01/2024
18/2023	Objeto: Pregão Eletrônico: Aquisição de Software, Microsoft 365 e **Antivírus**	925859	14/12/2023
5/2023	Objeto: Pregão Eletrônico: Contratação de empresa especializada para eventual fornecimento de licenciamento de **antivírus** Kaspersky para compor prateleira de produtos e serviços a serem comercializados pela PRODAM a seus clientes e consumidos pela própria PRODAM, conforme especificações detalhadas no Termo de Referência, constante do Anexo I, deste Instrumento convocatório.	927131	13/07/2023

Tabela 2 - Apêndice III - Análise de Projetos Similares - Solução de segurança do tipo detecção e resposta estendida.

Pregão	Unidade de Fornecimento	UASG - Unidade Gestora	Data da Compra
11/2023	CONTRATAÇÃO DE LICENÇAS DE SOFTWARE ANTIMALWARE, ANTISPAM, SEGURANÇA AVANÇADA PARA SERVIDORES E ENDPOINT, CONTEMPLANDO CONTRATAÇÃO DE OPERAÇÃO DE SERVIÇOS DE SEGURANÇA E ATUALIZAÇÃO DE VERSÕES, RELEASES E PATCHS DE CORREÇÃO POR PERÍODO DE 12 MESES	254420	24/04/2023

Apêndice IV - Pesquisa de itens no Catálogo de Materiais e Serviços (CATMAT/CATSER)

Por meio de pesquisa textual no catálogo de compras pública, disponível em: <https://catalogo.compras.gov.br/>, identificamos os códigos CATMAT/CATSER, relacionado na tabela a seguir o qual entendemos como os mais apropriados para a pretensa contratação.

Tabela 1 - Apêndice IV - Pesquisa de itens no Catálogo de Materiais e Serviços (CATMAT/CATSER).

Item	CATMAT/CATSER	Unidade de medida
Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software	27502	Unidade

Documento assinado eletronicamente por **OSMAR DA SILVA FERREIRA - Matr.1680990-4**, **Analista em Gestão e Assistência Pública à Saúde**, em 02/02/2024, às 09:31, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **ANDERSON JESUS DE MENEZES - Matr.1716623-3**, **Coordenador(a) Especial de Tecnologia de Informação em Saúde**, em 02/02/2024, às 14:40, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **FABIO AYUB BRASIL - Matr.1686557-X**, **Gerente de Atendimento**, em 02/02/2024, às 14:50, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **ALICE JULIANA XIMENES DE PONTES - Matr.1711083-1**, **Diretor(a) de Governança em Tecnologia da Informação**, em 02/02/2024, às 17:25, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

A autenticidade do documento pode ser conferida no site: http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 verificador= **131642195** código CRC= **09BD4768**.