AGENCIA NACIONAL DE SAUDE SUPLEMENTAR/RJ

Estudo Técnico Preliminar 12/2026

1. Informações Básicas

Número do processo: 33910.010765/2025-19

2. Descrição da necessidade

2.1 A descrição da solução como um todo, conforme minudenciado neste Estudo Preliminar, abrange a prestação do serviço de implementação, serviço gerenciado de administração, suporte técnico *on-site*, repasse de conhecimento *hands-on*, garantia e atualização por 24 (vinte e quatro) meses para a solução centralizada ou em nuvem de segurança do tipo endpoint protection (Antivírus/Antimalware) no âmbito da ANS.

2.2 O serviço deve ser provido por meio da implantação de tecnologia que possua capacidade de gerenciar de forma centralizada ou em nuvem os clientes instalados nas estações de trabalho, utilizando-se de licença de *software* com função de Antivírus, Anti-*Spyware*, Anti-Ransomware, EDR (Endpoint Detection and Response), *Firewall*, Proteção Contra Intrusos (HIPS), Controle de Dispositivos, Controle de Aplicações, Proteção contra ameaças de dia zero (zero-day), IDS (Intrusion Detection System), entre outras.

Os sistemas operacionais contemplados são:

A) Sistemas Linux:

- Amazon Linux
- Opensuse 13.10
- Solaris 10 U8
- Oracle Linux 6, 7, 8 e 9 (64-bit)
- Red Hat Enterprise Linux 4, 7, 8 e 9 (64-bit)
- CentOS 7 e 9 (64-bit)
- Debian GNU/Linux 10 (64-bit)
- SUSE Linux Enterprise Server 11 e 12 SP5 (64-bit)
- openSUSE 13.1 Bottle (64-bit)
- Other 3.x or later Linux (64-bit)
- Other Linux (64-bit)
- Ubuntu Linux (64-bit)

B) Sistemas Microsoft Windows:

- Microsoft Windows Server 2012, 2016, 2019 e 2022 (64-bit)
- Microsoft Windows 10 (64-bit)

2.3 O endpoint a ser adquirido deve ser minimamente compatível com os sistemas operacionais listados anteriormente, garantindo pleno funcionamento e suporte adequado a cada um deles.

2.4 Além disso, é imprescindível que ofereça compatibilidade com o Secure Boot e demais mecanismos de segurança, permitindo seu funcionamento simultâneo sem a necessidade de desativação ou comprometimento

de qualquer camada de proteção nativa. A solução deve garantir que as políticas de segurança sejam mantidas ativas, sem impacto na inicialização, operação ou atualização dos sistemas suportados.

2.5 Deverá suportar os ambientes em contêineres, atendendo minimamente as seguintes plataformas e tecnologias relacionadas:

2.5.1 OrchestrationPlatforms

- AWS Elastic Kubernetes Service (EKS);
- EC2 container service (EC2 ECS);
- Azure Kubernetes Service (AKS);
- Azure Web App;
- IBM Cloud Kubernetes Service (IKS);
- Rancher Kubernetes Engine (RKE);
- Google Kubernetes Engine (GKE);
- K3s;
- Kubernetes;
- OpenShift;
- Rancher;

2.5.2Container Runtime

- Containerd;
- Docker;
- CRI-O;

2.5.3 Network Plugins

- AWS VPN CNI;
- Kubenet;
- Azure CNI;
- Calico;
- Flannel;
- OpenShift SDN (OVS);
- OVN-Kubernetes;
- Canal.

2.5.4 Ainda com relação aos ambientes de Containers a solução deverá ter os seguintes recursos:

- Capacidade de analisar vulnerabilidades e configurações incorretas antes da implantação;
- Monitoramento contínuo para detectar e bloquear atividades maliciosas em containers em execução;
- Uso de inteligência artificial, análise de comportamento e regras customizáveis;
- Aplicação de políticas de segurança para restringir execução de processos não autorizados;
- Capacidade de validar compliance com normas como LGPD, ISO 27001 e CIS Benchmarks, por exemplo;
- Compatibilidade com plataformas de gerenciamento de eventos de segurança e automação de resposta.

2.6 As licenças que serão ativadas nos servidores de gerência deverão ser flutuantes entre, no mínimo, dois nós em *cluster* e caso isso não seja possível, cada um dos componentes deve ser licenciado para que as funcionalidades permaneçam ativas no caso de indisponibilidade de um dos nós.

2.7 A solução que suportará os serviços deve ainda ser implantada no datacenter da ANS, localizado no Rio de Janeiro, em ambiente virtualizado, sendo que na gerência da solução que for implantada no datacenter deverá fornecer proteção de 2.250 *endpoints*. Ainda neste contexto, a implantação dos serviços deve contemplar a desinstalação completa de quaisquer soluções similares atualmente existentes nas estações de trabalho da ANS.

2.8 Em resumo os serviços devem ser entregues de modo a prover segurança na camada de usuário e servidores, mitigando riscos capazes de impactar a produtividade dos colaboradores da Agência e degradar o desempenho dos sistemas e redes corporativas.

2.9 Fazem parte da contratação, visando a efetiva operacionalização e funcionamento das respectivas soluções:

2.9.1Licenciamento, implantação e configuração da solução;

2.9.2 Garantia e Atualização por 24 (vinte e quatro) meses;

2.9.3 Serviço Gerenciado de Administração, Operação e Suporte da Solução por 24 (vinte e quatro) meses;

2.9.4 Treinamentos aos usuários;

2.9.5 Repasse de conhecimento.

O objeto desse estudo encontra-se previsto no PGC 2026 – Planejamento e Gerenciamento de Contratações – e no PDTIC – Plano Diretor de Tecnologia da Informação e Comunicação, conforme quadro abaixo:

ATUALIZAR AS INFORMAÇÕES ABAIXO

Alinhamento estratégico

Id	Cód. PDTI	Objetivo Estratégico
1	3	Modernizar a infraestrutura de TIC e garantir a continuidade do negócio para a ANS

Id	Cód. PDTI	Metas
1.1	M5	Manutenção de Infraestrutura de TI

Id	Cód. PDTI	Necessidades Elencadas no PDTI (Ações)

1.1.1	M5-A2	Sustentação Operacional da Infraestrutura

ALINHAMENTO AO PAC 2025				
Nº do item	**Tipo item**	**Descrição**	**Código do item**	**Unidade Responsável**
28	Serviço de TIC	OUTROS SERVICOS PARA A INFRAESTRUTURA DE TECNOLOGIA DA INFORMACAO E COMUNICACAO (TIC)	27090	GETI

3. Área requisitante

Área Requisitante	Responsável
COMAG/GETI	Luciene Pinheiro Capra

4. Necessidades de Negócio

4.1 A Agência Nacional de Saúde Suplementar - ANS, possui um parque tecnológico que mantém informações estratégicas referentes aos planos, beneficiários e operadoras de planos de saúde, e todos os dados de processamentos de pesquisas de mercado e demais informações do mercado de planos de saúde suplementar do país.

4.2 Além disso, a segurança dos sistemas de informação tem revelado uma importância cada vez maior. Assim, urge ter sempre presente o nível de segurança desta instituição pública e a tomada de medidas visando uma melhor garantia de autenticidade, confidencialidade, integridade e disponibilidade dos sistemas.

4.3 A facilidade de comunicação com a rede mundial de computadores, coloca as instituições públicas, como a ANS, em um risco, ininterrupto, de infecção das estações de trabalho e servidores por malwares.

4.4 Com o intuito de mitigar os riscos é ativado o monitoramento de endpoints o qual é responsável por manter todos os dispositivos protegidos de maneira automática, bloquear ações indesejadas e ter um gerenciamento centralizado das estações de trabalho e, com isso, reportar sempre que houver um incidente.

4.5 A presente contratação visa minimizar a vulnerabilidade dos sistemas corporativos, redes, computadores servidores e microcomputadores, implementando metodologias de segurança de antivírus corporativo. Ademais, prevenir possíveis ataques internos e externos de vírus, spams e spywares e outras ameaças virtuais aos serviços de informações disponibilizados pela ANS.

4.6 Atualmente, devido a uma incompatibilidade com o endpoint em uso, tem sido necessário desabilitar o serviço de Secure Bot em alguns cenários. Ressaltamos nossa preocupação com a manutenção desse serviço desativado, uma vez que sua ausência pode comprometer a segurança do ambiente.

4.7 Diante disso, e considerando a impossibilidade de renovação do contrato de atualização das licenças de antivírus da ANS, torna-se essencial a contratação de uma solução centralizada de segurança do tipo Endpoint Protection (Antivírus /Antimalware). Essa solução deve atender à demanda atual e à projeção de crescimento do parque tecnológico nos próximos anos, garantindo a proteção dos ativos de TIC contra as diversas ameaças (malware) mencionadas.

4.8 Podemos citar que os principais benefícios esperados, além de todos os já citados, incluem a redução do número de ataques bem-sucedidos de vírus a servidores e estações a serviço da ANS, a elevação do nível de satisfação dos clientes do ambiente de TI e usuários de estações de trabalho e a redução de microcomputadores infectados.

5. Necessidades Tecnológicas

5.1 Para atender as necessidades da ANS, a solução de TI deve possuir uma plataforma única integrada de segurança, abrangendo solução de endpoint para estações de trabalhos e servidores físicos e virtuais, que deverá ser fornecida por um único fabricante de modo que tanto o suporte à solução quanto suas funcionalidades sejam inteiramente integradas e gerenciadas através de uma única console de gerenciamento.

5.2 A solução deve ser, preferencialmente, de um único fabricante de software, de modo que todas as funcionalidades sejam inteiramente integradas e gerenciadas através de um único console de gerenciamento. A solução deve conter um único agente instalado por endpoint, gerenciando todas as funções e comunicações com o console de gerenciamento.

5.3 A solução não pode depender de interfaces ou equipamentos intermediários entre o agente e o console de gerenciamento.

5.4 Deve ser composta por uma console de administração on-premise ou em nuvem, solução de Next Generation Anti-malware (NGA) e sistema de detecção e resposta de endpoint (EDR).

5.5 ealizar análise de comportamentos com base nas táticas, técnicas e procedimentos (TTPs) listados no framework MITREATT&CK. Fornecer proteção contra, no mínimo, os seguintes tipos de malwares: vírus, trojans, exploits, worms de rede, spywares, bots, ransomwares, adwares e toolkits .

5.6 Possibilitar a criação de whitelists e blacklists configuráveis pela contratante, de forma que se possa permitir ou bloquear a execução de um programa, independente do comportamento analisado pela inteligência da solução.

5.7 Além da detecção em memória e unidades de armazenamento locais do endpoint, a solução deve realizar, no mínimo, detecção em dispositivos periféricos conectados via USB e CDROM.

5.8 A solução deve suportar comunicação através de protocolo TCP-IP com suporte a IPV4 e IPV6. Durante a vigência do contrato, a contratada deve disponibilizar à contratante, sem nenhum custo adicional, novas versões e/ou correções na medida em que forem liberadas pelo fabricante da solução.

5.9 Todos os componentes da solução devem ser contemplados por serviço de suporte técnico especializado, para dirimir dúvidas e solucionar problemas técnicos que ocorrerem durante o uso da solução.

5.10 A contratada deve fornecer informações sobre como a contratante terá acesso ao serviço de suporte técnico para abertura de chamados e sobre como obter atualizações da solução.

5.11A solução deve reter informações (logs) de auditoria do console de administração e informações (logs) geradas nos endpoints, como, por exemplo: histórico de detecções de eventos e de atualizações.

5. 12 Deve permitir o download ou exportação dos logs gerados na console de gerenciamento.

5.13 O período de retenção deve contemplar, no mínimo, 30 dias, independente do volume de dados produzidos.

5.14 A solução deve possibilitar ser incluída em imagem padrão de desktop permitindo, assim, que novos equipamentos preparados já contenham a solução instalada em sua produção.

5.15 A solução deve possibilitar que sua instalação e remoção nos endpoints sejam realizadas por meio de, no mínimo, GPO's (Group Policy Objects) e/ou scripts.

5.16 Tais ações devem ocorrer sem obrigar a reinicialização dos endpoints.

5.17 Requisitos do console de Administração da solução deve ser centralizado, on-premise ou em nuvem do fabricante da solução com modelo de uso SaaS (Software-as-a-Service), e gerenciar todos os endpoints, independentemente de sua localização geográfica.

5.18 Deve estar acessível em regime integral (24x7), com disponibilidade mínima de 99% no mês.

5.19 Indisponibilidades no console para atualizações ou correções devem ser informadas à contratante com, pelo menos, 7 dias de antecedência e deverão ocorrer fora do horário comercial da contratante, exceto em casos de comprovada urgência.

5.20 É responsabilidade da contratada o gerenciamento e administração do hardware, sistema operacional e dos componentes necessários para manutenção da disponibilidade.

5.21 As mudanças necessárias nos endpoints com relação a políticas ou a atualizações devem ocorrer em conformidade com as configurações definidas pela contratante no console de administração, ou disparadas sob demanda, também por meio do console de administração.

5.22 Deve permitir o acesso ao console via internet, sendo compatível com, ao menos, o navegador Google Chrome.

5.23 O acesso ao console de administração deve ser criptografado com algoritmos que não sejam publicamente reconhecidos como inseguros.

5.24 Deve possibilitar o uso de duplo fator de autenticação para logon no console de administração da solução.

5.25 Deve suportar a definição de perfis de acesso com base em funções e/ou ações permitidas ou negadas dentro da solução, de forma que usuários possam ser vinculados a um perfil de acesso.

5.26 A solução deve possibilitar a criação de contas de usuários distintas, utilizando uma chave (por exemplo: nome de usuário, endereço de email, dentre outros), de forma que se possa identificar, inequivocamente, a autoria de ações na solução.

5.27.As contas criadas devem poder ser vinculadas a pelo menos um perfil de acesso previamente criado.

5.28 Deve registrar, para fins de auditoria, as ações realizadas pelos usuários do console de administração, sejam eles administradores ou não.

5.29 Deve possibilitar, a partir do console de administração, a atualização da solução, o gerenciamento de políticas e configurações dos agentes instalados nos endpoints.

5.30 Deve exibir a lista de endpoints que possuam a solução instalada, contendo, no mínimo, informações como: nome do endpoint, versão dos componentes instalados, última comunicação com o console, data de atualização, último evento de detecção de malware e endereço IP.

5.31 Deve possibilitar o agrupamento de endpoints, no mínimo, por Unidade Organizacional ou tipo de equipamento, possibilitando maior flexibilidade na aplicação e distribuição de configurações.

5.32 Deve permitir a gestão de todos os endpoints de forma unificada.

5.33 Deve permitir a criação ou configuração de dashboards, com utilização de tabelas ou gráficos, contendo, pelo menos, informações relacionadas:

5.34 Ao nível de atualização do ambiente, podendo-se observar o status de atualização dos componentes da solução nos endpoints. Às detecções e ações de resposta executadas.

5.35 À auditoria de ações dos administradores. Deve ter capacidade de produzir e exportar relatórios, ao menos, no formato PDF.

5.36Deve ter capacidade de enviar e-mails a partir da ocorrência de eventos de detecção ou com base em relatórios/consultas em datas e horários previamente configurados, para endereços eletrônicos definidos.

5.37 Deve operar analisando a execução da ameaça em potencial, nas camadas do Sistema Operacional e Memória, prevenindo a entrada de códigos maliciosos.

5.38 Deve utilizar tecnologias preditivas como Inteligência Artificial e Machine Learning para identificar e tratar ameaças conhecidas e desconhecidas, mesmo que o endpoint esteja desconectado da internet.

5.39 Possuir capacidade de extrair características dos arquivos potencialmente perigosos e aplicar algoritmos de análise para determinar sua intenção. Prover proteção contra ameaças conhecidas e desconhecidas.

5.40 Identificar e bloquear, no mínimo, a execução de binários, scripts, exploits ou comandos maliciosos, em tempo real. Identificar e bloquear ameaças avançadas (APTs), zero-day, LotL e ransomwares , em tempo real.

5.41 Os módulos de proteção de memória e controle de execução devem prevenir, no mínimo, as seguintes técnicas de ataques: Hijacking, File injection, File Overflow, In-Memory execution, Explotation, Process Injection, Escalation;

5.42 Detectar e prevenir qualquer alteração oriunda de código malicioso ou não-autorizado, em programas que estejam sendo executados em memória.

5.43.A proteção de memória, em caso de violação, deve possuir, pelo menos, as ações de Alertar, Bloquear, Terminar, ou equivalentes.

5.44 O controle e análise de scripts deve ser capaz de analisar, no mínimo, scripts em PowerShell, javascript, vbscript e Active Scripts possibilitando, pelo menos, as ações de alertar e bloquear, ou equivalentes.

5.45 Caso ocorra alguma identificação de código malicioso em scripts, a ferramenta deve prevenir sua execução imediata.

5.46 Deve possibilitar detecção, no caso de execução, em tempo real, de malwares contidos em arquivos compactados, no mínimo, nos formatos ZIP, 7z, RAR, EXE, ARJ e CAB.

5.47 A análise do malware deve ocorrer em pré-execução, ou seja, o código malicioso deve ser bloqueado antes de ser executado e infectar o endpoint .

5.48 No processo de detecção e bloqueio em pré-execução não serão aceitas tecnologias que dependam do uso de vacinas ou assinaturas.

5.49 Caso seja identificado um programa malicioso, a sua execução não deve ser permitida.

5.50 Deve ser capaz de finalizar processos e subprocessos em execução caso haja a identificação de algum código malicioso sendo executado nos mesmos.

5.51 Possuir mecanismos contra a desinstalação ou desativação não autorizada. Possuir serviço de proteção contra finalização (kill) do processo da solução.

5.52 Também deve impedir que outros aplicativos efetuem a finalização do serviço.

5.53Todas as funcionalidades da solução devem ser ativadas por um único produto, facilitando a instalação, a configuração e o gerenciamento.

5.54 Deve ser compatível, no mínimo, os seguintes sistemas operacionais:

Sistemas Linux:

- Amazon Linux
- Opensuse 13.10
- Solaris 10 U8
- Oracle Linux 6, 7, 8 e 9 (64-bit)
- Red Hat Enterprise Linux 4, 7, 8 e 9 (64-bit)
- CentOS 7 e 9 (64-bit)
- Debian GNU/Linux 10 (64-bit)
- SUSE Linux Enterprise Server 11 e 12 SP5 (64-bit)
- openSUSE 13.1 Bottle (64-bit)
- Other 3.x or later Linux (64-bit)
- Other Linux (64-bit)
- Ubuntu Linux (64-bit)

Sistemas Microsoft Windows:

- Microsoft Windows Server 2012, 2016, 2019 e 2022 (64-bit)
- Microsoft Windows 10 (64-bit)

5.55 É imprescindível que ofereça compatibilidade com o Secure Boot e demais mecanismos de segurança, permitindo seu funcionamento simultâneo sem a necessidade de desativação ou comprometimento de qualquer camada de proteção nativa.

5.56 Deverá suportar os ambientes em contêineres.

5.57 Deve gerar e armazenar registros (logs) dos eventos de detecção de ameaças;

5.58 Possibilitar a notificação de eventos de ameaças através de alerta via syslog ou por e-mail.

5.59 Aceitar parâmetros de configuração e distribuição como, pelo menos, instalação silenciosa, personalização de pastas de destino e personalizações nas funcionalidades/configurações a serem instaladas, sem necessidade de reiniciar o endpoint.

5.60 Deve ser reconhecida pelo Windows como solução de proteção anti-malware ou equivalente.

5.61 Requisitos da solução de Detecção e Resposta para Endpoints (EDR): Deve permitir analisar o comportamento e ações relacionadas ao ataque malicioso.

5.62 Centralizar as informações no console central quando houver necessidade de análise, investigação ou pesquisa, desonerando o endpoint da carga de tal processamento.

5.63 Possibilitar a consolidação automática de alertas relacionados a diversos endpoints em um único incidente.

5.64 Permitir visualizar em modo gráfico, através do console web, linha de tempo contendo a sequência de eventos que ocorreram durante a execução do malware ou do evento, possibilitando, ainda, o detalhamento de cada evento, elencando as táticas e técnicas utilizadas.

5.65 Possibilitar a criação de telas ou relatórios sobre as detecções de ameaças com, no mínimo, as seguintes informações: nome do processo, conexões de rede, operações com chaves de registro, consultas DNS realizadas.

5.66 Permitir a monitoração contínua dos eventos, com captura e gravação em modo seguro.

5.67Manter as informações relacionadas aos eventos maliciosos e investigações por pelo menos 30 dias.

5.68 Identificar conexões de rede suspeitas, com origem e destino.

5.69 Permitir visibilidade para o movimento lateral em todo o parque de endpoints.

5.70 Possuir capacidade para isolar ou bloquear o endpoint na rede de computadores.

5.71 Possuir capacidade de executar ação automática previamente configurada na ocorrência de uma epidemia no ambiente tecnológico.

5.72 Possuir a capacidade de prevenção de perda de dados (DLP) para plataformas de colaboração e comunicação, como Office 365, Teams e e-mail.

5.73Possuir a disponibilidade para a instalação em dispositivos moveis, incluindo celulares ou tablets, tanto Android quanto iOS.

5.74 A contratada deverá fornecer treinamentos aos usuários desta agência, com os seguintes objetivos:

5.74.1Fomentar o desenvolvimento de uma cultura organizacional mais consciente e preparada para enfrentar os desafios da segurança digital moderna.

5.74.2 Atender à crescente necessidade de comportamentos seguros no ambiente digital.

5.75 O programa de treinamento deve incluir uma ampla gama de tópicos, como reconhecimento de phishing, proteção de dados, práticas para criar senhas seguras e identificação de ameaças internas e externas.

5.76 Os materiais devem ser interativos e dinâmicos, incluindo simulações de ataques reais e vídeos instrutivos, com o intuito de aumentar o engajamento dos participantes e facilitar a retenção do conhecimento.

5.77 A utilização de uma abordagem baseada em cenários reais e exemplos práticos reforçará o aprendizado, incentivando a aplicação das lições no cotidiano profissional.

5.78 Com isso, a solução contribuirá significativamente para a formação de uma cultura organizacional mais informada e resiliente em relação à segurança digital.

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

6.1 Requisitos de capacitação

6.1.1 A CONTRATADA deverá realizar o serviço gerenciado de administração e o repasse de conhecimento aos funcionários da CONTRATANTE que atuarão, em conjunto, com a solução de segurança adquirida, abrangendo todas as informações necessárias à sua operacionalização, disponibilizando materiais em mídias digitais, apostilas e outros recursos em português brasileiro, bem como realizar todo e qualquer treinamento, das equipes indicadas pela contratante, que sejam necessários ao pleno conhecimento do funcionamento da solução e de sua gerência.

6.2 Requisitos de manutenção e continuidade dos serviços

6.2.1Inicialmente, todo atendimento será realizado via telefone (0800) ou Internet, salvo quando os especialistas da CONTRATADA julgarem necessária ou quando uma visita técnica for solicitada pela CONTRATANTE para solução de um problema. Nesses casos o atendimento deverá contar com a presença de um técnico especializado, representando a CONTRATADA, para resolver o problema. Os dias e horários de atendimento obedecerão a conveniência da ANS;

6.2.2 É autorizado que o serviço de suporte técnico seja fornecido pela fabricante da solução, desde que não haja prejuízos à ANS no atendimento e desde que sejam obedecidas todas as especificações constantes para fornecimento do serviço;

6.2.3 O Suporte deverá ser especializado, podendo ser executado remotamente ou localmente dependendo da criticidade ou dificuldade. A avaliação do chamado quanto a criticidade será feita pela ANS.

6.2.4 A CONTRATADA deverá manter cadastro de, no mínimo 06 (seis), colaboradores indicados pela Gerência de Tecnologia de Informação - GETI - com permissão para, em seu nome, abrir chamados de assistência técnica e utilizar os serviços de suporte;

6.2.5A documentação produzida durante a execução dos serviços, seja em papel ou meio eletrônico, será de propriedade do CONTRATANTE e não deverá ser divulgado sem sua expressa autorização.

6.3 Requisitos Legais

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

6.3.2 Lei nº 8.248, de 23 de outubro de 1991 - Dispõe sobre a capacitação e competitividade do setor de informática e automação, e dá outras providências;

6.3 3 Instrução Normativa SEGES/ME Nº 81, de 25 de novembro de 2022 - Dispõe sobre a elaboração do Termo de Referência - TR, para a aquisição de bens e a contratação de serviços, no âmbito da administração pública federal direta, autárquica e fundacional, e sobre o Sistema TR digital;

6.3.4 Instrução Normativa SEGES Nº 58, de 8 de agosto de 2022 - Dispõe sobre a elaboração dos Estudos Técnicos Preliminares - ETP, para a aquisição de bens e a contratação de serviços e obras, no âmbito da administração pública federal direta, autárquica e fundacional, e sobre o Sistema ETP digital;

6.3.5 Instrução Normativa SEGES/ME nº 77, de 4 de novembro 2022 - Dispõe sobre a observância da ordem cronológica de pagamento das obrigações relativas ao fornecimento de bens, locações, prestação de serviços e realização de obras, no âmbito da Administração Pública federal direta, autárquica e fundacional;

6.3.6 Instrução Normativa SEGES Nº 73, de 30 de setembro de 2022 - Dispõe sobre a licitação pelo critério de julgamento por menor preço ou maior desconto, na forma eletrônica, para a contratação de bens, serviços e obras, no âmbito da Administração Pública federal direta, autárquica e fundacional;

6.3.7 Instrução Normativa SEGES/ME Nº 26, de 13 de abril de 2022 - Dispõe sobre a dispensa, o parcelamento, a compensação e a suspensão de cobrança de débito resultante de multa administrativa e/ou indenizações, previstas na Lei nº 14.133, de 1º de abril de 2021, no âmbito da Administração Pública federal direta, autárquica e fundacional, não inscritas em dívida ativa;

6.3.8 Instrução Normativa nº 5, de 25 de maio de 2017, da, então, Secretaria de Gestão do Ministro do Planejamento, Desenvolvimento e Gestão/MPDG - Dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta;

6.3.9 Instrução Normativa nº 49, de 30 de junho de 2020 - Altera a Instrução Normativa nº 5, de 26 de maio de 2017, que dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional.

6.3.10 Decreto nº 11.246, de 27 de outubro de 2022 - Regulamenta o disposto no § 3º do art. 8º da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre as regras para a atuação do agente de contratação e da equipe de apoio, o funcionamento da comissão de contratação e a atuação dos gestores e fiscais de contratos, no âmbito da administração pública federal direta, autárquica e fundacional;

6.3.11 Decreto nº 10.947, de 25 de janeiro de 2022 - Regulamenta o inciso VII do caput do art. 12 da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre o plano de contratações anual e instituir o Sistema de Planejamento e Gerenciamento de Contratações no âmbito da administração pública federal direta, autárquica e fundacional.

6.3.12 bDecreto-Lei nº 200, de 25 de fevereiro de 1967 - Dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências;

6.3.13 Decreto nº 9.507, de 21 de setembro de 2018 - Dispõe sobre a execução indireta, mediante contratação, de serviços da administração pública federal direta, autárquica e fundacional e das empresas públicas e das sociedades de economia mista controladas pela União;

6.3.14 Decreto nº 3.555, de 8 de agosto de 2000 - Aprova o Regulamento para a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns;

6.3.15 Decreto nº 7.845, de 14 de novembro de 2012 - Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

6.3.16 Portaria SEGES/ME nº 938, de 2 de fevereiro de 2022 - Institui o catálogo eletrônico de padronização de compras, serviços e obras, no âmbito da Administração Pública federal direta, autárquica e fundacional, em atendimento ao disposto no inciso II do art. 19 da Lei nº 14.133, de 1º de abril de 2021;

6.3.17 Portaria nº 443, de 27 de dezembro de 2018 - Estabelece os serviços que serão preferencialmente objeto de execução indireta, em atendimento ao disposto no art. 2º do Decreto nº 9.507, de 21 de setembro de 2018;

6.3.18 Resolução Administrativa – RA Nº 81, de 2 de maio de 2023 e suas alterações – Dispõe sobre a Política de Segurança da Informação da Agência Nacional de Saúde Suplementar.

6.4 Requisitos Sociais, Ambientais e Culturais

6.4.1 Uma vez que o objeto da pretensa contratação consiste, essencialmente, em prestação de serviços à própria infraestrutura de TI da Agência Nacional de Saúde Suplementar, naquilo que couber, os serviços,

resultados, relatórios, catálogos, gráficos, prospectos, demonstrativos, entre outros inerentes a serem fornecidos deverão ter documentação (catálogos, manuais, informativos e afins) entregue em Língua Portuguesa (Brasil), e excepcionalmente de comum acordo em Língua Inglesa, e na forma de links de acesso ao sitio de documentação da própria ANS, base de conhecimento, sistema de Wiki, outro que venha a ser definido por esta Agência.

6.5 Requisitos de Segurança da Informação

6.5.1 Seguir a Política de Segurança da Informação da ANS, ou equivalente, aderente ao disposto na IN GSI/PR nº 1, de27 de maio de 2020, incluindo políticas ou normas para proteção de dados pessoais vigentes e atualizadas. A CONTRATADA deverá garantir que todos os profissionais a seu serviço que estejam alocados para os serviços na ANS tenham conhecimento das Políticas da Segurança da Informação, da Lei Geral de Proteção de Dados Pessoais (LGPD) e demais normas que tratam do assunto.

6.5. 2 A CONTRATANTE se reserva o direito de realizar auditoria de Segurança da Informação e Privacidade (SIP) relativa à conformidade dos requisitos de segurança da informação e privacidade previstos pela contratação.

6.5.3 Deverá fornecer as soluções de acordo com as políticas de segurança da informação da ANS, inclusive no que tange a registros de log e controle criptográficos, possibilitar a rastreabilidade de forma a manter trilha de auditoria de SIP. Deverá também definir um processo de gestão de riscos de SIP que envolvam a solução de TIC.

6.5.4 A CONTRATADA deverá restituir imediatamente à CONTRATANTE, quando do término do serviço ou quando for solicitada, qualquer informação confidencial provinda da prestação dos serviços. Em caso de perda de quaisquer dessas informações, a CONTRATADA deverá notificar imediatamente por escrito;

6.5.5 A não observância do disposto sobre confidencialidade torna a PARTE infratora sujeita às penalidades cabíveis previstas em lei.

6.5.6 Devido à necessidade de acesso restrito para os serviços desta contratação, conforme descrito neste documento, será exigido os seguintes critérios:

1. Utilizar somente de pessoal capacitado para as atividades e regularmente contratados na forma da legislação trabalhista, observando-se ainda as disposições da Portaria 3435 /91 do MTPS (NR/17 - Ergonomia) e de convenções coletivas do trabalho celebradas entre os Sindicatos Patronais e de Empregados para as categorias profissionais envolvidas;
2. Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse da ANS ou de terceiros de que tomar conhecimento em razão da execução do contrato, respeitando todos os critérios estabelecidos neste termo, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes;
3. Cuidar e comunicar à Equipe de Segurança da Informação para que todos os privilégios de acesso a sistemas, informações e recursos da ANS sejam revistos, modificados ou revogados quando da transferência, remanejamento, promoção ou demissão de profissionais sob sua responsabilidade.

6.5.7 Implementar e manter, em conjunto com a CONTRATANTE, controles e procedimentos específicos para assegurar a segurança física e do ambiente de acesso às bases, informações, sistemas e demais ativos que compõem a Solução de TIC, de forma a prevenir qualquer tipo de ocorrência de evento de efeitos danosos ou prejudiciais ao funcionamento dos recursos de processamento das informações relacionadas à Solução de TIC, reduzindo assim o nível de risco ao qual o objeto do contrato e/ou a CONTRATANTE estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela CONTRATANTE.

6.5.8 Apresentar à CONTRATANTE, sempre que solicitado, toda e qualquer informação e documentação que comprovem a implementação dos requisitos de SIP especificados na contratação, de forma a assegurar a auditabilidade continuada do objeto contratado, bem como demais dispositivos legais aplicáveis.

6.5.9 Realizar, em conjunto com a CONTRATANTE, ou com outros órgãos por ela indicados, ações de tratamento de incidentes de SIP relacionados ao objeto do contrato, bem como apoiar essas ações com o monitoramento e o envio de informações tempestivos.

6.5.10 Será exigido que a empresa providencie para os coordenadores/supervisores técnico/preposto, certificado digital (A3) com base no padrão ICP-Brasil para assinatura dos documentos digitais, conferindo integridade e autenticidade na troca de informações entre a ANS e a CONTRATADA para atender ao fluxo dos processos eletrônicos na aplicação (SEI) implantada na contratada.

6.6 Requisitos de adequação a Lei Geral de Proteção de dados Pessoais (LGPD)

6.6.1 Cumprir o que se dispõe na Lei Geral de Proteção de Dados Pessoais (LGPD) nº 13.709/2018, realizando o tratamento de informações classificadas e proteção de dados pessoais, por parte dos colaboradores na execução deste serviço. A CONTRATADA também deverá seguir as orientações da RESOLUÇÃO ADMINISTRATIVA – RA Nº 81, DE 13 DE MARÇO DE 2023, ou versões atualizadas posteriormente, referente à Política de Segurança da Informação da ANS.

6.6.2 Evitar vazamento de informações mantendo sigilo e privacidade, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse da ANS ou de terceiros de que tomar conhecimento em razão da execução do contrato, respeitando todos os critérios estabelecidos neste termo, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes.

6.6.3 Implementar e manter controles e procedimentos específicos para assegurar completo e absoluto sigilo quanto a todos os dados e informações de que o preposto ou os demais empregados da CONTRATADA venham a tomar conhecimento em razão da execução do contrato, deforma a assegurar que seus empregados e outros profissionais sob sua direção e/ou controle respeitem o uso dos dados somente para as finalidades previstas em contrato e as restrições de uso dos ativos utilizado para desenvolvimento e/ou operação da Solução de TIC, cumprindo e fazendo cumprir o disposto nos Termo de Compromisso e Ciência e Termo de responsabilidade e sigilo firmados respectivamente, pelo representante legal e pelo(s) empregado(s) da CONTRATADA.

6.6.4 Definir e executar procedimento de descarte seguro dos dados pessoais ou sigilosos da CONTRATANTE ao encerrar a execução do contrato.

6.6.5 Realizar, em conjunto com a CONTRATANTE, análise de impacto na privacidade dos dados pessoais relacionada à Solução de TIC, considerando o descrito pelo relatório de impacto à proteção de dados pessoais, conforme previsto na Lei nº 13.709/2018, quando da concepção de qualquer novo projeto, produto ou serviço.

6.6.6 Implementar controles de acesso baseados em uma política de controle de acesso para o objeto contratado, elaborada pela CONTRATANTE em conjunto com a CONTRATADA, tendo em vista o princípio do menor privilégio, a segurança da informação e a privacidade, de forma a reduzir o nível de risco ao qual o objeto e a CONTRATANTE estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela CONTRATANTE.

6.6.7 A política deve estabelecer, dentre outros critérios, que se deve conceder autorizações de acesso apenas quando realmente sejam necessárias para o desempenho de uma atividade específica, definindo também protocolos para cadastramento, mecanismo de controle de acesso (como, por exemplo, validação de formulário), habilitação, inabilitação, atualização de direitos de acesso e exclusão de usuário, além de revisões periódicas da política.

6.6.8 A política também deve definir situações e protocolos para acesso a informações sensíveis, necessidades de não repúdio, situações que requerem autenticação via duplo fator e acesso via certificado digital, nos casos em que a CONTRATANTE julgar necessário.

6.6.9 Utilizar recursos de segurança da informação e de tecnologia da informação de qualidade, eficiência e eficácia reconhecidas e em versões comprovadamente seguras e atualizadas, de forma reduzir o nível de risco ao qual o objeto do contrato e/ou a CONTRATANTE está exposta, considerando os critérios de aceitabilidade de riscos definidos pela CONTRATANTE.

6.6.10 Reportar de imediato à CONTRATANTE incidentes que envolvam vazamento de dados, indisponibilidade ou comprometimento da informação relacionados à Solução de TIC, processamento não autorizado ou outro não cumprimento dos termos e condições contratuais. O tratamento de incidentes de segurança da informação será realizado através da ferramenta de gestão de incidentes da ANS;

6.7 Requisitos de garantia

6.7.1 A CONTRATADA garantirá os serviços realizados dentro do escopo desta contratação durante a vigência do contrato. Deverá a Contratada, no período de garantia, realizar todas as correções decorrentes dos erros ou falhas cometidas na execução dos serviços, no menor tempo possível, sem qualquer custo a CONTRATANTE.

7. Estimativa da demanda - quantidade de bens e serviços

7.1 Para subsidiar a nova contratação da solução de ANTIVÍRUS por esta Agência, a COMAG, responsável pelo processo, fundamentou-se no gerenciamento da solução atualmente em uso, que conta com 2.000 licenças adquiridas. Conforme registrado no documento SEI 31780260, a utilização em janeiro de 2025 foi de 1.895 licenças.

7.2 Considerando a necessidade de atender à demanda vigente e prever futuras expansões, optou-se por ampliar a contratação de 2.000 para 2.250 licenças. Essa decisão leva em conta a expectativa de ingresso de aproximadamente 293 novos servidores, decorrente de um concurso público a ser realizado, conforme confirmado pelo RH no documento SEI XXXX (ANEXAR E_MAIL DO RH LEVANTAMENTO). Além disso, a ampliação visa garantir margem para a aquisição de novos notebooks e desktops, bem como para eventuais expansões na infraestrutura de servidores da ANS, assegurando a proteção contínua e escalável dos ativos de TI da Agência.

7.3 Em relação ao item 2, o Repasse de Conhecimentos refere-se à transferência de competências por parte da contratada à equipe da contratante, com foco no gerenciamento de toda a solução implementada. Já o treinamento será disponibilizado a todos os usuários da agência, com o objetivo de promover o desenvolvimento de uma cultura organizacional mais consciente e preparada para enfrentar os desafios da segurança digital contemporânea, atendendo à crescente demanda por comportamentos seguros no ambiente digital.

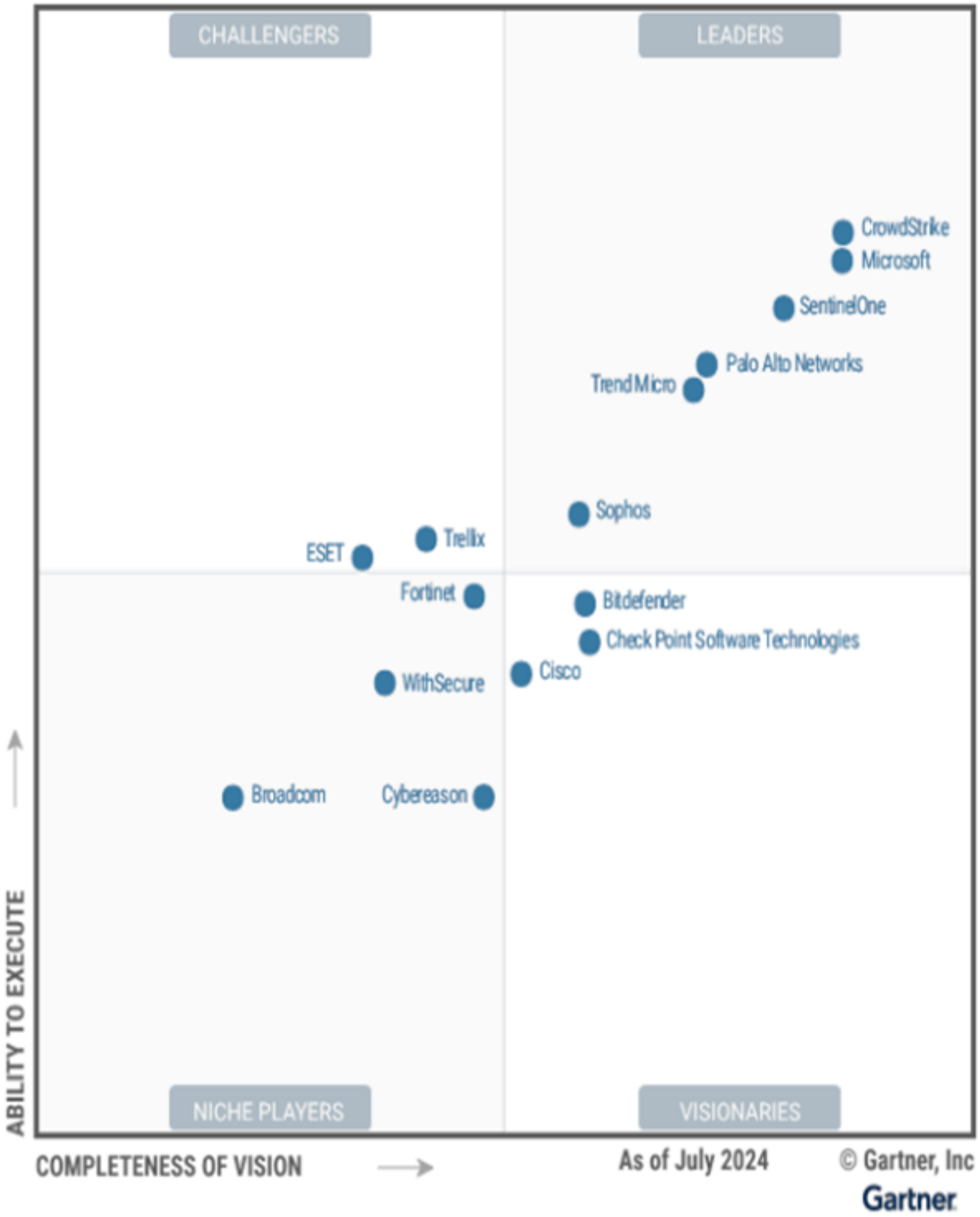
ITEM	DESCRIÇÃO	QUANTIDADE
1	Solução centralizada de segurança do tipo endpoint protection (Antivírus/Antimalware).	2250 Unidades
2	Serviço Gerenciado deAdministração, Operação e Suporteda Solução do item 1, Implantação da solução, Repasse de conhecimento e Treinamento.	24 meses

8. Levantamento de soluções

8.1 O mercado de soluções de segurança com gerência centralizada para controle de ameaças em estações de trabalho apresenta diversos fabricantes e soluções conforme pode ser visto em levantamento anual realizado pelo Gartner (Figura 1), acerca de soluções centralizadas de antivírus.

Magic Quadrant

Figure 1: Magic Quadrant for Endpoint Protection Platforms



8.2 Para demonstrar a viabilidade técnica e econômica de uma solução centralizada de antivírus corporativo, foram analisados 4 (quatro) cenários distintos. No CENÁRIO 1, tomamos como referência a contratação existente, ajustando o número das licenças para **2.250** assim como seu período, para **24 meses**. No CENÁRIO 2, utilizamos como base a aquisição de **300 (trezentas) licenças de antivírus e EDR** realizada pelo Conselho Regional de Engenharia e Agronomia da Bahia (CREA-BA) para um período de **36 meses**. No **Cenário 4**, a aquisição envolve um volume maior de licenças: **3.200 de antivírus e XDR (Extended Detection and Response)**, realizada pelo **Poder Judiciário, especificamente pelo Supremo Tribunal Federal (STF)**. Assim como no cenário anterior, o contrato tem duração de **36 meses**.

8.3 Com base nessas referências, ajustamos o número de licenças para **2.250**, assim como o período, para **24 meses**, que é a quantidade necessária para atender às demandas identificadas pela ANS, permitindo assim uma estimativa proporcional dos custos de aquisição.

8.4 Para os cenários restantes, buscamos cotações diretas junto aos fabricantes ou representantes das soluções consideradas.

ANS				
CUSTO TOTAL DE PROPRIEDADE: ANÁLIS PARA O CENÁRIO 1				
ITEM	DESCRIÇÃO	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Solução centralizada de segurança do tipo endpoint protection (Antivírus/Antimalware)	2250	R$ 96,80	R$ 217.800,00
2	Serviço Gerenciado de Administração, Operação e Suporte da Solução do item 1	24	R$ 1.833.33	R$ 44.000,00
			TOTAL:	R$ 261.800,00

CONSELHO REG. DE ENGENHARIA E AGRONOMIA-BA - PREGÃO ELETRÔNICO Nº 90013/2024-000				
CUSTO TOTAL DE PROPRIEDADE: ANÁLIS PARA O CENÁRIO 2				

ITEM	DESCRIÇÃO	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	licenças de solução antivírus e EDR por um período de 24 meses com instalação e treinamento.	2250	R$ 397,89	R$ 895.252,50
			TOTAL:	R$ 895.252,50

BLUE EYE				
CUSTO TOTAL DE PROPRIEDADE: ANÁLIS PARA O CENÁRIO 3				
ITEM	DESCRIÇÃO	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Solução de EDR - Endpoint Detection and Response, Symantec SESC	2250	R$ 323,30	R$ 727.449,75
2	Serviço de implementação e suporte mensal da solução	24	R$ 12.500,00	R$ 300.000,00
			TOTAL:	R$ 1.027.449,75

PODER JUDICIÁRIO SUPREMO TRIBUNAL FEDERAL - PREGÃO ELETRÔNICO Nº 90005/2024				
CUSTO TOTAL DE PROPRIEDADE: ANÁLIS PARA O CENÁRIO 4				
ITEM	DESCRIÇÃO	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Fornecimento de subscrições de solução de detecção e resposta estendida a incidentes de segurança cibernética - XDR (eXtended Detection and Response)	2250	R$ 670,00	R$ 1.507.500,00

2	Serviços de monitoramento, prevenção, detecção e resposta a ameaças de nova geração, contemplando operação, gestão, suporte e atualizações da solução XDR (eXtended Detection and Response)	24	R$ 3.568,35	R$ 85.640,40
3	Treinamento	1	R$ 31.823,33	R$ 31.823,33
			TOTAL:	R$1.542.891,68

9. Análise comparativa de soluções

Solução 1 - ANS	
Fabricante:	Blackberry
Descrição:	Antivírus CylancePROTECT
Análise da Solução:	A ANS utiliza o Cylance, desenvolvido pela Blackberry, há cerca de três anos. Atualmente, o Cylance está instalado em mais de 1.900 endpoints da ANS. No entanto, a solução CylancePROTECT tem causado problemas de degradação de desempenho em alguns servidores Linux. Infelizmente, a fabricante não tem se mostrado proativa na resolução deste problema.

Solução 2 - PREGÃO ELETRÔNICO Nº 90013/2024-000	
Fabricante:	Kaspersky
Descrição:	Antivírus Kaspersky Next EDR Optimum
Análise da Solução:	A Kaspersky Next EDR Optimum é projetada para fornecer proteção robusta contra ameaças cibernéticas avançadas através de funcionalidades de Endpoint Detection and Response (EDR). Ela combina a capacidade de detectar, investigar e responder a incidentes de segurança em tempo real, facilitando a identificação de comportamentos suspeitos e ameaças complexas. Não foram feitas análises dessa solução, apenas uma cotação dos valores para referência do mercado.

Solução 3 – Blue Eye	
Fabricante:	Symantec
Descrição:	Antivírus Symantec SESC
Análise da Solução:	O Symantec Endpoint Security é a versão totalmente gerenciada na nuvem do Symantec, que fornece proteção de várias camadas para impedir as ameaças, independentemente de como eles atacam os endpoints. Não foram feitas análises dessa solução, apenas uma cotação dos valores para referência do mercado.

Solução 4 - PREGÃO ELETRÔNICO Nº 90005/2024	
Fabricante:	Crowdstrike
Descrição:	Endpoint Security
Análise da Solução:	A solução CrowdStrike Falcon oferece proteção avançada para endpoints com sua solução de detecção e resposta estendida a incidentes de segurança cibernética - XDR (eXtended Detection and Response),sendo amplamente reconhecida por sua eficácia em prevenir, detectar e responder a ameaças cibernéticas em tempo real. Não foram feitas análises dessa solução, apenas uma cotação dos valores para referência do mercado.

10. Registro de soluções consideradas inviáveis

10.1 Após análise detalhada das opções disponíveis para proteção de endpoints, foi considerado inviável continuar a utilizar a solução CylancePROTECT, fornecida pela Blackberry, como parte do nosso plano de segurança cibernética. Apesar de estar em uso na ANS há aproximadamente três anos, com instalação em mais de 1.900 endpoints, a solução tem apresentado problemas significativos. Especificamente, foram identificadas ocorrências de degradação de desempenho em alguns servidores Linux, afetando a eficiência operacional dos nossos sistemas.

10.2 Além dos problemas identificados com a solução anterior, a análise da alternativa denominada solução 2 evidenciou outro gap crítico: a ausência de um serviço de gerenciamento integrado. Sem esse recurso, a administração centralizada e o monitoramento contínuo das políticas de segurança ficam comprometidos, exigindo intervenções manuais constantes e aumentando o risco de falhas operacionais. Em função dessa limitação, a solução 2 não pré-configura os mecanismos indispensáveis para uma gestão eficiente e responsiva do ambiente, o que a torna inviável para atender aos rigorosos padrões e às demandas crescentes de segurança cibernética da organização.

11. Análise comparativa de custos (TCO)

11.1.A análise de Custo Total de Propriedade (TCO – Total Cost Ownership) é um instrumento utilizado para analisar e subsidiar a escolha dasolução sob o aspecto de custos estimado durante o ciclo de vida de cada solução.

1. **Mapa comparativo dos cálculos totais de propriedade (TCO)**

DESCRIÇÃO	Fabricante	Solução	Valor Anual	Valor Bianual
SOLUÇÃO VIÁVEL 3	Symantec	Antivírus Symantec SESC	R$ 513.724,87	R$ 1.027.449,75
SOLUÇÃO VIÁVEL 4	Crowdstrike	Endpoint Security XDR	R$ 771.445,84	R$ 1.542.891,68

12. Descrição da solução de TIC a ser contratada

12.1 Considerando que a solução atual, CylancePROTECT, desenvolvida pela Blackberry, tem apresentado problemas significativos de degradação de desempenho e que a fabricante não demonstrou proatividade na resolução dessas questões, decidimos buscar uma nova solução de segurança. O objetivo é adquirir uma solução que ofereça gerenciamento centralizado ou em nuvem, proporcionando controle eficiente de ameaças em estações de trabalho.

12.2Este processo de contratação será conduzido com ampla concorrência de mercado, focando na obtenção do menor preço global, mas garantindo que a proposta selecionada ofereça o melhor valor para a administração, atendendo aos requisitos tecnológicos mínimos especificados no item 5 deste documento.

12.3 Portanto, recomendamos a aquisição de uma solução centralizada de segurança do tipo endpoint protection (Antivírus/Antimalware) para a Agência Nacional de Saúde Suplementar - ANS. Esta solução deve incluir serviços de implementação, gerenciamento, suporte técnico on-site, transferência de conhecimento hands-on, treinamentos aos usuários de toda a agência, com garantia e atualizações por um período de 24 (vinte e quatro) meses.

13. Estimativa de custo total da contratação

Valor (R$): 1.027.449,75

TOTAL ANUAL Valor (R$): 513.724,87.

Valor total dos 24 meses (R$): 1.027.449,75.

BLUE EYE
CUSTO TOTAL DE PROPRIEDADE: ANÁLIS PARA O CENÁRIO 3

ITEM	DESCRIÇÃO	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Solução centralizada de segurança do tipo endpoint protection (Antivírus/Antimalware).	2250	R$ 323,30	R$ 727.449,75
2	Serviço Gerenciado de Administração, Operação e Suporte da Solução do item 1, Implantação da solução, Repasse de conhecimento e Treinamento.	24	R$ 12.500,00	R$ 300.000,00
			TOTAL:	R$ 1.027.449,75

14. Justificativa técnica da escolha da solução

14.1 A solução de segurança atualmente em uso, o CylancePROTECT, desenvolvida pela Blackberry, revelou-se inadequada devido a problemas de desempenho significativos. A degradação na performance de alguns servidores, associada à falta de respostas da fabricante para corrigir as falhas, comprometeu a eficiência da Agência Nacional de Saúde Suplementar (ANS). Essa situação motivou a busca por uma nova solução que garanta não apenas a proteção efetiva, mas também a continuidade e eficiência nas operações da ANS.

14.2 Em decorrência da análise realizada, a escolha de uma nova solução de antivírus não é apenas necessária, como fundamental para garantir a continuidade das atividades da ANS com segurança e eficiência. A adoção de uma solução que atenda aos requisitos técnicos e operacionais requisitados, aliada a um processo de ampla concorrência para assegurar as melhores condições comerciais, representa um avanço significativo na estratégia de segurança cibernética da agência. A implementação desta solução é um passo essencial na proteção dos dados e na infraestrutura crítica da ANS, alinhando-se às melhores práticas e exigências do setor de saúde suplementar.

14.3 Dessa forma, a contratação será abordada com ampla concorrência de mercado e menor preço global, auferindo a proposta com o valor mais vantajoso para a administração, desde que atendam aos requisitos mínimos tecnológicos elencados no item 5 deste documento. Destarte, recomendamos a aquisição de solução centralizada ou em nuvem de segurança do tipo endpoint protection (Antivírus/Antimalware) no âmbito da Agência Nacional de Saúde Suplementar - ANS, incluindo serviços de implementação, serviço gerenciado de administração, suporte técnico on-site, repasse de conhecimento hands-on, treinamentos aos usuários de toda a agência, com garantia e atualizações por um período de 24 (vinte e quatro) meses.

15. Justificativa econômica da escolha da solução

15.1 A presente contratação estará aberta as empresas parceiras dos diversos fabricantes que entregam soluções de segurança com gerência centralizada ou em nuvem para controle de ameaças em estações de trabalho. Dessa forma, a contratação será abordada com ampla concorrência de mercado e menor preço global, auferindo a proposta com o valor mais vantajoso para a administração, desde que atendam aos requisitos mínimos tecnológicos elencados no item 5 deste documento.

16. Benefícios a serem alcançados com a contratação

16.1 Continuar oferecendo Infraestrutura de TI adequada para que as áreas finalísticas do negócio da ANS continuem operacionais;

16.2 Contribuir para garantia de um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos;

16.3 Oferecer maior agilidade e eficácia no tratamento de incidentes envolvendo endpoints (estações de trabalho e notebooks) comprometidos;

16.4 Evitar, mitigar e conter a propagação de pragas digitais facilitando o tratamento destes incidentes (vírus /malwares/spywares, spam, entre outros) com a administração centralizada da solução de proteção;

16.5 Permitir o controle de acesso à rede por dispositivos computacionais, permitindo gerenciamento destes dispositivos;

16.6 Gerar economicidade e melhoria de qualidade do serviço de proteção de endpoints;

16.7 Mitigar riscos de infecção na transição entre soluções de antivírus.

17. Providências a serem Adotadas

17.1 A Administração tomará as seguintes providências previamente ao contrato:

- Definições dos servidores que farão parte da equipe de fiscalização e gestão contratual;
- Capacitação dos fiscais e gestores a respeito do tema objeto da contratação;
- Definição de planos de trabalho com vistas à boa execução contratual;
- Acompanhamento rigoroso das ações previstas nos projetos apresentados.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

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

19. Responsáveis

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

EUNICIO LAINA SOARES

Integrante Requisitante

NADIA VENDRUSCOLO PIONER

Integrante Requisitante

Assinou eletronicamente em 02/07/2026 às 09:13:35.

JORGE EDUARDO VIEIRA

Integrante Técnico

Assinou eletronicamente em 02/07/2026 às 10:06:45.

MARCOS REGES REIS RIBEIRO SEGUNDO

Integrante Técnico

RAFAEL PEREIRA SARDINHA

Integrante Requisitante

ITALA BINES

Integrante Administrativo

LUCIENE PINHEIRO CAPRA

Autoridade Máxima da Área de TIC

Assinou eletronicamente em 03/07/2026 às 16:24:14.