Estudo Técnico Preliminar

1. Informações Básicas

Número do processo: 02070.003600/2022-45

2. Descrição da necessidade

2.1 **Necessidade da Contratação**

2.1.1 Atualmente, com 334 (trezentas e trinta e quatro) Unidades de Conservação, o Instituto possui uma estrutura institucional apoiada por aproximadamente 3000 (três mil) colaboradores lotados nas diversas Unidades distribuídas em todo o território nacional, equipes que atuam nos 754.599,30 km² (setecentos e cinquenta e quatro mil, quinhentos e noventa e nove, vírgula trinta centésimos de quilômetros quadrados), de áreas protegidas de responsabilidade do Governo Federal.

2.1.2 A segurança da rede do ICMBio depende da utilização de recursos de segurança cibernética, que dentro das suas várias camadas de proteção está a aferição do comportamento de estações de usuários e de servidores com o fito de proteção contra ameaças básicas e avançadas.

2.1.3 A aferição do comportamento das estações de usuários e servidores de rede tem como objetivo a detecção, bloqueio, investigação e resposta a incidentes de segurança da informação que venham porventura ocorrer no âmbito da rede do ICMBio, tendo como alvo ou mesmo vetor de contaminação e execução um dos equipamentos plugados na rede.

2.1.4 O ICMBio possui um amplo parque computacional para atendimento aos usuários. Atualmente existem mais de 3000 usuários ativos na rede do ICMBio, de acordo com as licenças de suíte de escritório atribuídas aos servidores e colaboradores do Instituto.

2.1.5 O parque de servidores de rede físicos presentes no CPD do ICMBio necessita de uma camada a mais de proteção visando a proteção contra ameaças básicas e avançadas em seus serviços de TIC. Portanto, é essencial que os servidores de rede estejam plenamente protegidos.

2.1.6 As fontes de contaminação por pragas digitais vão desde a invasão da rede por um elemento mal intencionado, que explora vulnerabilidades de rede e computadores, até o próprio comportamento do usuário do ICMBio, que mesmo sem intenção e de forma inocente, pode ser o vetor de um ataque realizado por elementos inescrupulosos. As principais fontes de contaminação são o acesso à internet, pendrives, e-mail, serviços disponibilizados ao público externo e interno, VPN´s de usuários, dentre outras.

2.1.7 Desta forma, faz-se necessário prover o ICMBio de recursos de segurança atualizados que possam monitorar e atuar em caso de contaminação por software criados por elementos mal intencionados e inescrupulosos, cujo objetivo vai desde a uma simples exposição da informação obtida até a exigência de valores para a liberação do que foi sequestrado, como é o caso de ataques por Ransomware.

2.1.8 Cabe reforçar que o Instituto não possui uma ferramenta atual de antivírus. Visando sanar esse 'gap', utiliza-se hoje no ICMBio, como uma solução paliativa, o Windows Defender pertencente ao Sistema Operacional Windows. Entretanto, essa solução não é eficaz assim como é uma solução robusta de endpoint, o que aumenta o potencial de invasão na rede do ICMBio.

3. Área requisitante

Área Requisitante	Responsável
Coordenação de Tecnologia da Informação e Comunicação	Marcelo Orrico de Souza

4. Necessidades de Negócio

4.1 Requisitos de Negócio

4.1.1 Solução de proteção contra ameaças avançadas, com funcionalidades de detecção, bloqueio, investigação e resposta a incidentes, incluindo console Web ou console gráfica do próprio fabricante para administração da solução e centralização de eventos.

4.1.2 Fornecimento da console de gerência, incluindo implantação dos agentes, documentação da arquitetura da solução e treinamento.

4.1.3 Garantia de atualização e Suporte da solução pelo prazo de 36 (trinta e seis) meses, prorrogáveis por mais 12 (doze) meses.

4.1.4 A solução de gerência deve ser fornecida pela licitante vencedora e contemplar todos os softwares e respectivas licenças necessárias ou adicionais para a instalação, configuração e funcionamento da solução de proteção. A licença, garantia e suporte da solução devem ser mantidas operacionais, mesmo que, em virtude do recebimento definitivo, esta ultrapasse a vigência contratual.

4.1.5 A solução de proteção deve ser oferecida na última versão disponibilizada pelo fabricante. Na data da proposta, nenhum dos softwares componentes da solução de proteção ofertados poderão estar listados pelo fabricante com data definida para fim de suporte (“end of support”) ou fim de vendas (“end of sale”).

5. Necessidades Tecnológicas

5.1 Agentes da Solução

5.1.2 Os agentes da solução devem ser compatível com as versões de Sistema Operacionais:

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

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

5.1.2.2 Para servidores de rede físicos ou virtuais:

I - Microsoft Windows Server 2012 (64bit) ou superior.

II - Ser suportado em sistemas operacionais Linux (32-64bit)

III - O agente deve suportar sua instalação em Sistemas Operacionais virtualizados em ambiente Vmware ou Hyper-V.

5.2 Consoles de Gerenciamento

5.2.1 A solução deve oferecer console de gerência via protocolo web seguro ou console do próprio fabricante.

5.2.2 Caso a console seja Web, deve ser compatível com pelo menos dois dos seguintes navegadores: Microsoft Edge 41 ou superior; Google Chrome 70 ou superior; Mozilla Firefox 60 ou superior.

5.2.3 A console deve funcionar plenamente sem requerer a instalação de plug-ins, drivers, java e flash player.

5.2.4 Permitir no mínimo 5(cinco) acessos simultâneos.

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

6.1 Requisitos Legais

6.1.1 Lei n° 8.666, de 21 de junho de 1993, que institui normas para licitações e contratos da Administração Pública.

6.1.2 Decreto nº 8.540, de 9 de outubro de 2015, estabelece, no âmbito da administração pública federal direta, autárquica e fundacional, medidas de racionalização do gasto público nas contratações para aquisição de bens e prestação de serviços e na utilização de telefones celulares corporativos e outros dispositivos.

6.1.3 Lei n° 10.520, de 17 de julho de 2002, que institui modalidade de licitação denominada pregão, para contratação/aquisição de bens e serviços comuns.

6.1.4 Lei n° 8.248, de 23 de outubro de 1991, que dispõe sobre a capacitação e competitividade do setor de informática e automação.

6.1.5 Decreto n° 3.555, de 08 de agosto de 2000, que aprova o regulamento para a modalidade de licitação denominada pregão, para contratação/aquisição de bens e serviços comuns.

6.1.6 Decreto n° 5.450, de 31 de maio de 2005, que regulamenta o pregão, na forma eletrônica, para contratação/aquisição de bens e serviços comuns.

6.1.7 Decreto lei 9.760/2019, de 11 de abril de 2019, que alterou o Decreto nº 6.514, de 22 de julho de 2008.

6.1.8 Decreto nº 7.174, de 12 de maio de 2010, que regulamenta a contratação de bens e serviços de informática e automação pela Administração Pública Federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União.

6.1.9 Na forma do art. 3º, inciso III, do Decreto nº 7.174, de 12 de maio de 2010, a CONTRATADA deverá apresentar no momento da entrega do objeto, a comprovação da origem dos bens importados oferecidos e da quitação dos tributos de importação a eles referentes.

6.1.10 Instrução Normativa nº 73, de 5 de Agosto de 2020, dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.

6.1.11 Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

6.1.12 Portaria STI/MP n° 20, de 14 de junho de 2016, que dispõe sobre orientações para contratação de soluções de Tecnologia da Informação no âmbito da Administração Pública Federal direta, autárquica e fundacional e dá outras providências.

6.2 Requisitos de Capacitação

6.2.1 A Contratada deverá realizar um treinamento para até 15 pessoas do ICMBio da solução a ser instalada, contemplando instalação, parametrização, monitoramento, melhores práticas e atuação de incidentes.

6.2.2 O treinamento deverá ser realizado na modalidade presencial nas dependências do ICMBio, localizada em Brasilia - DF, podendo ser transmitido de forma remota a participantes a serem definidos pelo ICMBio.

6.2.3 O material do treinamento elaborado pela Contratada deverá ser fornecido em língua portuguesa. Caso seja utilizado material elaborado exclusivamente pelo fabricante e fique demonstrado que este não é oferecido em língua portuguesa, será aceito o fornecimento em língua inglesa.

6.2.4 O treinamento deve conter parte teórica e prática, incluindo tópicos sobre a instalação, uso, configuração, resolução de problemas da solução, análise de relatórios, respostas a incidentes, introdução ao Framework MITRE ATT&CK e outros.

6.2.5 As datas do treinamento devem ser previamente combinadas com o ICMBio.

6.2.6 Todas as despesas do treinamento devem correr por conta da Contratada.

6.2.7 Deverá ser disponibilizado formulário de avaliação (online ou impresso) e a média das notas deverá ser superior a 80%. Caso a media da notas seja inferior a 80% a contratada deverá ministrar novo treinamento.

6.2.8 A fornecedora e/ou fabricante da solução poderá, a qualquer tempo, durante a vigência do contrato, sem ônus extra para o ICMBio, oferecer participação em seminários, conferências, visitas técnicas, eventos educacionais e treinamentos não previstos nesta especificação técnica, desde que relacionados ao objeto contratado.

6.3 Requisitos e funcionalidades técnicos da solução

6.3.1 A solução de proteção deve ser capaz de 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.

6.3.2 A solução de proteção deverá possuir funcionalidades especificas para prevenção contra a ação de ransomwares com capacidade, em caso de incidente de restauração dos arquivos comprometidos.

6.3.3 A solução de proteção deve ter a funcionalidade específica de impedir as técnicas de manipulação e randomização de memória impossibilitando a exploração de vulnerabilidades em aplicações.

6.3.4 A solução de proteção deve ter a capacidade de impedir os ataques direcionados mesmo que utilizando as vulnerabilidades de dia zero, mitigando no mínimo os conhecidos comportamentos de exploração de vulnerabilidades.

6.3.5 Efetuar a 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.

6.3.6 Realizar análise de comportamento com base nas táticas, técnicas e procedimentos (TTPs) listados no framework MITREATT&CK.

6.3.7 A análise dos artefatos deve ocorrer em pré-execução, ou seja, antes de serem executados no sistema operacional, evitando que a máquina seja infectada.

6.3.8 Detectar e bloquear ameaças que utilizem técnicas de ofuscação e sequestro de DLL.

6.3.9 Detectar e bloquear técnicas de evasão, incluindo process injection e uso de executáveis legítimos do Windows para rodar scripts e ações maliciosas.

6.3.10 Reconhecer padrões e bloquear comportamentos potencialmente maliciosos ou o possuir mecanismos automáticos preventivos ou corretivos que sejam capazes de inibir as ações maliciosas resultantes de pelo menos 5(cinco) das ações listadas abaixo:

6.3.10.1 Rodar a partir diretórios incomuns (ex: diretório de dados, temp e lixeira);

6.3.10.2 Executar elevações de privilégio inesperadas;

6.3.10.3 Tentar se passar por processos do Windows;

6.3.10.4 Estabelecer conexões de rede suspeitas (call back ou command & control);

6.3.10.5 Uso suspeito do PSEXEC;

6.3.10.6 Invocação maliciosa através do Rundll;

6.3.10.7 Exploração ou modificação do arquivo hosts;

6.3.10.8 Tentativa de invocação de Remote Shell.

6.3.10.9 Identificar e bloquear alterações suspeitas em chaves de registro e tarefas agendadas na máquina.

6.3.10.10 Proteger contra macros maliciosas, bem como scripts e comandos Powershell maliciosos.

6.3.10.11 Bloquear exploits e payloads suspeitos do Metasploit.

6.3.11 As análises poderão ser complementadas utilizando recursos em nuvem da solução, sem custos adicionais, onde será permitido apenas o envio de metadados dos artefatos sob análise, sem submissão do artefato em si ou seu conteúdo à nuvem.

6.3.12 O agente da solução deve realizar suas análises e bloqueios nas estações mesmo quando estiver sem conectividade com os servidores da solução e sem acesso à Internet.

6.3.13 O agente da solução deve possuir proteção contra desinstalação e/ou desativação dos seus componentes, serviços e processos de forma não autorizada.

6.3.14 Deve ser possível realizar a configuração de proxy no agente ou obter as configurações de proxy definidas no próprio sistema operacional.

6.3.15 Deve ser possível exibir ou inibir alertas ao usuário em caso de detecção de alguma ameaça, conforme definição do administrador.

6.3.16 Deve ser possível definir as seguintes ações de resposta quando uma ameaça ou comportamento malicioso for detectado:

6.3.16.1 Ignorar;

6.3.16.2 Registrar em log;

6.3.16.3 Alertar;

6.3.16.4 Bloquear;

6.3.16.5 Remover ou quarentenar;

6.3.16.6 Isolar a máquina, 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.

> I - O agente deve ter a capacidade de fazer o isolamento da máquina por si só, sem precisar de nenhuma integração com outros softwares ou dispositivos de rede para isso.
>
> II - Deve ser possível ao administrador efetuar a liberação da máquina do isolamento via console de gerência ou fornecer uma chave para realizar a liberação.

6.3.17 A solução deve possuir funcionalidade de 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.

6.3.18 A console deve oferecer uma 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.

6.3.19 Devem ser coletadas as atividades de todos artefatos analisados, contendo informações sobre interação com outros processos, arquivos e chaves de registro acessadas/modificadas, conexões de rede realizadas, dentre outras.

6.3.20 A solução deve correlacionar os eventos de detecção e bloqueio de malwares, permitindo sua visualização na console.

6.3.21 Deve ser possível configurar regras de exclusão (whitelists) determinando quais arquivos, diretórios, processos ou aplicativos não devem ser analisados pela solução.

6.3.22 A solução deve ser capaz de remover de forma ágil e eficaz outras soluções de antivírus instaladas nos equipamentos do ICMBio ou possuir mecanismos que possibilitem essa remoção.

6.3.23 A Solução deve ter a capacidade de implementar, no mínimo, cinco das seguintes funcionalidades:

6.3.23.1 Reputação de Arquivos (Com ou sem acesso à internet no endpoint);

6.3.23.2 IPS de Próxima Geração;

6.3.23.3 Proteção de Navegadores;

6.3.23.4 Aprendizado de Máquinas;

6.3.23.5 Análise Comportamental;

6.3.23.6 Mitigação da Exploração de Memória;

6.3.23.7 Controle e isolamento de determinadas aplicações;

6.3.23.8 Controle de Dispositivos;

6.3.23.9 Emulação para Malware;

6.3.23.10 Proteção ao ambiente de Active Directory;

6.3.23.11 Mitigação de Exploração de Vulnerabilidades em aplicações conhecidas.

6.3.24 Deve ter a capacidade de implementar a funcionalidade de “Machine Learning” utilizando como fonte de aprendizado a rede de inteligência do fabricante, correlacionando no mínimo as seguintes técnicas de proteção com os vetores de ataques, identificando não somente os aspectos maliciosos.

6.3.25 De forma opcional ou não obrigatória a solução poderá ser capaz de distribuir iscas no ambiente com o objetivo de detectar e interromper tentativas de infiltração, através da implementação de pelo menos:

6.3.25.1 Criação de entradas falsas de cache, como Cache de DNS afim de enganar um invasor e identificar ações maliciosas no ambiente;

6.3.25.2 Deve possibilitar a criação de arquivos falsos nas máquinas dos usuários;

6.3.25.3 Deve possibilitar a criação e distribuição de senhas falsas nos sistemas afim de identificar invasores no ambiente;

6.3.25.4 Criação de compartilhamentos de rede falsos em desktops;

6.3.25.5 Deve ser capaz de enviar alertas quando as “Iscas” falsas são acionadas e/ou modificadas;

6.3.25.6 Deve ter a capacidade de revelar tentativas de ataques dentro da rede interna;

6.3.26 De forma opcional ou não obrigatória, a solução poderá ter a capacidade de impedir os ataques direcionados mesmo que utilizando as vulnerabilidades de dia zero, mitigando no mínimo um dos conhecidos comportamentos de exploração de vulnerabilidades:

6.3.26.1 SEHOP - Structured Exception Handler Overwrite Protection;

6.3.26.2 Heap Spray (Exploits que iniciam através do HEAP);

6.3.26.3 Java Exploit Protection;

6.3.27 De forma opcional ou não obrigatória, a solução poderá se capaz de:

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

6.3.27.2 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;

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

6.3.27.4 A solução poderá ser capaz de identificar vulnerabilidades, erros de configurações e possíveis Backdoors presentes no Active Directory;

6.3.27.5 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;

6.3.27.6 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;

6.4 Instalação dos agentes:

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

6.4.2 Deve 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.

6.4.3 A instalação deve ser feita de forma silenciosa, sem interação com o usuário e sem necessidade de acesso à Internet.

6.4.4 Deve ser possível permitir a desinstalação ou alteração da configuração do agente mediante requisição de senha ou token gerados pela console de gerência.

6.4.5 Deve ser possível impedir alterações na configuração do agente por usuários ou processos não autorizados.

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

6.4.7 Para equipamentos que não podem se conectar à internet, devido a regras de negócio e/ou restrições impostas pelo próprio equipamento, a solução deve possibilitar a instalação do agente on-premise, para que tais equipamentos possam ser gerenciados, atualizados e protegidos.

6.4.8 Toda a solução deverá funcionar com agente nas estações de trabalho e servidores físicos e/ou virtuais a fim de diminuir o impacto ao usuário final. Será permitido agentes múltiplos para o atendimento deste requisito.

6.5 Console de Gerência:

6.5.1 A console e os agentes da solução devem possuir interface em português ou inglês.

6.5.2 Toda comunicação da solução deve ocorrer de forma criptografada usando protocolo seguro conforme padrão aceito pela indústria.

6.5.3 Permitir a configuração de perfis com permissões agrupadas que possam ser vinculados às contas de acesso à solução, para possibilitar a segregação de funções.

6.5.4 Suporte à criação de usuários, permitindo senhas de no mínimo 8 caracteres de 3 ou mais tipos, como: letras maiúsculas, letras minúsculas, dígitos numéricos e caracteres especiais.

6.5.5 A solução de console de gerência, deve ser possível configurar autenticação em múltiplos fatores.

6.5.6 Permitir ao administrador criar diferentes políticas de segurança e aplicá-las a diferentes grupos de máquinas de acordo com seus atributos.

6.5.7 Registro em log de todas as ações de detecção e bloqueio de malware e comportamento malicioso.

6.5.8 Deve ser possível efetuar busca no log pelo IP de Origem, IP de destino, nome da máquina, nome do processo, arquivo e chave de registro.

6.5.9 Deve ser possível efetuar o “drill down” das consultas realizadas afim de avaliação mais detalhada das ocorrências.

6.5.10 A partir dos eventos exibidos na console, deve ser possível tomar ações como quarentenar a máquina, adicionar o artefato a blacklist ou lista de exclusão (whitelist), dentre outras.

6.5.11 Permitir a geração de relatórios, consulta em log ou dashboard para visualizar no mínimo as informações abaixo:

6.5.11.1 Eventos de ameaças;

6.5.11.2 Eventos de comportamentos suspeitos;

6.5.11.3 Malwares detectados e bloqueados;

6.5.11.4 Computadores infectados.

6.5.12 Deve ser possível exportar os relatórios para o formato CSV ou PDF.

6.5.13 Permitir a configuração de alertas em tempo real de ameaças com envio de e-mail a usuários pré-definidos.

6.5.14 A solução deve manter log de auditoria com registro das configurações realizadas por qualquer usuário ou administrador do sistema.

6.5.15 Permitir a visualização do inventário das máquinas que possuem o agente instalado, contendo no mínimo as seguintes informações:

6.5.15.1 Nome da máquina;

6.5.15.2 Endereço IP;

6.5.15.3 Versão do sistema operacional;

6.5.15.4 Versão do agente;

6.5.15.5 Política aplicada.

6.5.16 A partir do console de gerenciamento da solução, deve ser possível 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.

6.5.17 As ações de gerenciamento de eventos/incidentes, na console, poderá ser efetuada tanto pelo administrador, quando, preventivamente e de forma automática pela solução.

6.6 Instalação da solução

6.6.1 A disponibilização da solução de gerência e a instalação e configuração dos agentes da solução deverá ser realizada pela Contratada ou pelo fabricante da solução presencialmente na Sede do ICMBio em Brasília, em dias úteis, no período de 8h00 às 12h00 e de 14h00 às 18h00.

6.6.2 A disponibilização da solução de gerência e a instalação e configuração dos agentes da solução deve ser executada por pessoal especializado, qualificado e com certificação na solução.

6.6.3 A instalação compreenderá:

6.6.3.1 Implantação de todos os componentes em sua última versão estável.

6.6.3.2 Configuração completa da solução, incluindo o apoio na definição de políticas e melhores práticas de segurança.

6.6.3.3 Configuração de dashboards, relatórios e alertas, de maneira coordenada com o ICMBio.

6.6.3.4 Customização dos pacotes de instalação dos agentes e distribuição a todas as estações do ICMBio.

6.6.3.5 Instrução da equipe técnica do ICMBio para a integração da solução com ferramenta SIEM ou envio para servidor de registro de logs (Syslog).

6.6.3.6 Entrega da documentação da topologia da solução, relatório das atividades e configurações realizadas.

6.6.3.7 Apresentação da solução configurada e implantada.

6.7 Garantia

6.7.1 A Contratada deverá fornecer garantia de atualização da solução pelo prazo de 36 (trinta e seis) meses, prorrogáveis por mais 12 (doze) meses, contados a partir da data da emissão do Termo de Recebimento, não se limitando ao término da vigência contratual.

6.7.2 Deverá ser oferecido suporte da Contratada, com possibilidade de abertura de chamados de 7h00 às 20h00, nos dias comerciais, para resolução de problemas.

6.7.3 A Contratada deve escalar o chamado para o suporte do fabricante sempre que necessário, seja devido à criticidade, impacto ou urgência do problema, como também caso o fabricante precise atuar no processo de correção.

6.7.4 Deverá ser fornecido acesso ao site do fabricante para acompanhamento dos chamados, acesso à base de conhecimentos e a fóruns sobre a solução.

6.7.5 A garantia deverá prover, obrigatoriamente:

6.7.5.1 Atualização das versões dos softwares fornecidos, se novas versões forem disponibilizadas;

6.7.5.2 Atualização dos softwares fornecidos, se houver lançamento de novos softwares em substituição aos fornecidos, ou se, mesmo não se tratando de substituição, ficar caracterizada descontinuidade dos softwares fornecidos;

6.7.5.3 Correções dos softwares fornecidos (patches), incluindo a correção de eventuais falhas (bugs) de software que prejudiquem o ambiente de produção ou vulnerabilidades que comprometam a segurança da solução;

6.7.5.4 A garantia deverá ser prestada durante todo o período de contrato e aditivos relativos as a atualização das licenças e proteção.

6.7.6 As manutenções corretivas, por solicitação expressa do ICMBio à Contratada, e preventiva, por solicitação da Contratada ao ICMBio, serão realizadas dentro dos seguintes limites:

6.7.6.1 No caso de manutenções preventivas, o horário do atendimento deverá ser compreendido entre 8h00 e 18h00, em dias úteis;

6.7.6.2 No caso de manutenções corretivas, o horário do atendimento deverá ser compreendido entre 7h00 e 20h00, em dias úteis;

6.7.6.3 O início do atendimento não poderá ultrapassar:

I - O prazo de 2(duas) horas, contadas a partir da solicitação feita pelo ICMBio, no caso de problemas de alto impacto (São consideradas como “Alta” todas as falhas cujas consequências tenham impactos negativos, gerando indisponibilidade sobre o serviço. São situações que exijam atenção imediata. Exemplo: Situação de indisponibilidade total do serviço, funcionamento intermitente ou parcial, que possa levar à interrupção intermitente, parcial ou total de serviços da solução.);

II - O prazo de 4 (quatro) horas, contadas a partir da solicitação feita pelo ICMBio, no caso de problemas de médio impacto (Problemas que não prejudicam significativamente o funcionamento dos serviços. São problemas sérios ou perturbações, que afetam uma área específica ou determinada funcionalidade. Exemplo: Degradação de desempenho, perda de funcionalidades.); e

III - O prazo de oito (oito) horas, contadas a partir da solicitação feita pelo ICMBio, no caso de problemas de baixo impacto (Solicitação de informações sobre o funcionamento da solução, possíveis configurações ou usos, que não gerem interrupções, nem indisponibilidade de determinada área ou uma funcionalidade específica.).

6.7.6.4 O término da correção do problema não poderá ultrapassar:

I - O prazo de 24(vinte e quatro) horas, contadas a partir da solicitação feita pelo ICMBio, no caso de problemas de alto impacto;

II - O prazo de 48 (quarenta e oito) horas, contadas a partir da solicitação feita pelo ICMBio, no caso de problemas de médio impacto; e

III - O prazo de 72 (setenta e duas) horas, contadas a partir da solicitação feita pelo ICMBio, no caso de problemas de baixo impacto.

6.7.6.5 O ICMBio poderá solicitar o suporte local (on-site), em Brasília, para manutenção corretiva. Nesse caso, um técnico da Contratada deverá estar presente nas dependências do ICMBio em Brasília em até 4 (quatro) horas, contadas a partir da solicitação feita pelo ICMBio. O prazo de chegada do técnico será acrescentado ao prazo de solução, desde que não solicitado /autorizado para atendimento no início do dia seguinte.

6.8 Prazos para entrega e instalação da solução

6.8.1 A entrega das eventuais licenças ou termos de uso de softwares da solução deve ser realizada em até 30 (trinta) dias corridos, contados a partir da data da assinatura da ordem de serviço.

6.8.2 A solução deverá estar completamente disponibilizada, instalada, configurada e operacional em até no máximo 60(sessenta) dias, contados a partir da data de assinatura da ordem de serviço.

6.8.3 A garantia em caso de renovação contratual, por meio de termo aditivo, deverá ser prestada de forma automática, ou seja, não deverá sofre interrupção. Caso ocorra interrupção na atualização, sem justificativa deferida pela fiscalização, o atraso será contado em dias a partir do momento da interrupção.

6.9 Requisitos de Manutenção

6.9.1 A Contratada deverá fornecer garantia de atualização e suporte da solução pelo prazo de 36 (trinta e seis) meses, prorrogáveis por mais 12 (doze) meses, contados a partir da data da emissão do Termo de Recebimento Definitivo (TRD), não se limitando ao término da vigência contratual.

6.9.2 Deverá ser oferecido suporte da Contratada, com possibilidade de abertura de chamados de 7h00 às 20h00, nos dias comerciais, para resolução de problemas.

6.9.3 A Contratada deve escalar o chamado para o suporte do fabricante sempre que necessário, seja devido à criticidade, impacto ou urgência do problema, como também caso o fabricante precise atuar no processo de correção.

6.9.4 Deverá ser fornecido acesso ao site do fabricante para acompanhamento dos chamados, acesso à base de conhecimentos e a fóruns sobre a solução.

6.9.5 A garantia deverá prover, obrigatoriamente:

- Atualização das versões dos softwares fornecidos, se novas versões forem disponibilizadas;
- Atualização dos softwares fornecidos, se houver lançamento de novos softwares em substituição aos fornecidos, ou se, mesmo não se tratando de substituição, ficar caracterizada descontinuidade dos softwares fornecidos;
- Correções dos softwares fornecidos (patches), incluindo a correção de eventuais falhas (bugs) de software que prejudiquem o ambiente de produção ou vulnerabilidades que comprometam a segurança da solução;

6.9.6 As manutenções corretivas, por solicitação expressa do ICMBio à Contratada, e preventiva, por solicitação da Contratada ao ICMBio, serão realizadas dentro dos seguintes limites:

- No caso de manutenções preventivas, o horário do atendimento deverá ser compreendido entre 8h00 e 18h00, em dias úteis;
- No caso de manutenções corretivas, o horário do atendimento deverá ser compreendido entre 7h00 e 20h00, em dias úteis.

6.10 Requisitos Temporais

6.10.1 Na contagem dos prazos estabelecidos neste ETP, quando não expressados de forma contrária, excluir-se-á o dia do início e incluir-se-á o do vencimento.

6.10.2 Todos os prazos citados, quando não expresso de forma contrária, serão considerados em dias corridos (ou horas corridas, quando definido em horas).

6.10.3 O prazo de início da execução das Ordem de Serviço de Fornecimento será contado a partir do primeiro dia útil subsequente à data da entrega ao Preposto da CONTRATADA por qualquer meio formal de comunicação, salvo quando definida outra data pela CONTRATANTE na OS.

6.10.4 Os esclarecimentos solicitados pela fiscalização do contrato deverão ser prestados imediatamente pela CONTRATADA, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 6 (seis) horas úteis.

6.10.5 Não será computado o tempo de atraso quando este estiver sido ocasionado pela CONTRATANTE ou por fatos supervenientes que independam de ações da CONTRATADA, desde que devidamente justificado e aceito pela CONTRATANTE.

6.10.6 Não são considerados casos ou fatos supervenientes as situações externas que poderiam ter sido contornadas ou mitigadas por ações de logísticas preventivas ou reativas da CONTRATADA.

6.10.7 Os atendimentos de suporte e assistência técnica devem ser prestados na forma a ser indicado pela CONTRATADA, inclusive sobre a substituição de equipamentos quando necessário por motivo de defeito de fabricação.

6.11 Requisitos de Segurança e Privacidade

6.11.1 A CONTRATADA, por meio de seu representante legal ou preposto, deverá em até 10 (dez) dias corridos após a assinatura do contrato, assinar o Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes no ICMBio, conforme modelo apresentado no ANEXO A - TERMO DE COMPROMISSO do TR. Da mesma forma, todos os empregados da CONTRATADA diretamente envolvidos na contratação deverão assinar Termo de Ciência da citada declaração, conforme modelo apresentado ANEXO B - TERMO DE CIÊNCIA do TR.

6.11.2 Todas as informações, imagens, aplicativos e documentos providos pela CONTRATANTE ou oriundos das informações que forem propriedade da CONTRATANTE que forem manuseados e utilizados, são de propriedade da CONTRATANTE, não podendo ser repassadas, copiadas, alteradas ou absorvidas na relação de bens da CONTRATADA, bem como, de seus executores, sem expressa autorização da CONTRATANTE.

6.11.3 Será considerado ilícito a divulgação, o repasse ou utilização indevida de informações, bem como dos documentos, imagens, gravações e informações utilizados durante a prestação dos serviços.

6.11.4 A CONTRATADA obriga-se a dar ciência à CONTRATANTE, imediatamente e por escrito, sobre qualquer anormalidade que verificar na prestação dos serviços.

6.11.5 A CONTRATADA deverá guardar inteiro sigilo dos dados processados, reconhecendo serem estes de propriedade exclusiva da CONTRATANTE, sendo vedada à CONTRATADA sua cessão, locação ou venda a terceiros sem prévia autorização formal da CONTRATANTE, de acordo com os termos constantes do ANEXO A - TERMO DE COMPROMISSO do TR.

6.11.6 Todas as informações obtidas ou extraídas pela CONTRATADA quando da execução dos serviços deverão ser tratadas como confidenciais, sendo vedada qualquer reprodução, utilização ou divulgação a terceiros, devendo a CONTRATADA zelar

por si e por seus sócios, empregados e subcontratados pela manutenção do sigilo absoluto sobre os dados, informações, documentos, especificações técnicas e comerciais de que eventualmente tenham conhecimento ou acesso em razão dos serviços executados.

6.11.7 Os equipamentos deverão possuir acesso às correções disponibilizadas pelo fabricante, enquanto existir o suporte às versões fornecidas.

6.12 Requisitos Sociais, Ambientais e Culturais

6.12.1 Quanto aos requisitos sociais, os profissionais da CONTRATADA, quando nas dependências do ICMBio, deverão apresentar-se vestido de forma adequada ao ambiente de trabalho, evitando-se o vestuário que caracterize o comprometimento da boa imagem institucional do ICMBio.

6.12.2 Os profissionais também deverão respeitar todos os servidores, funcionários e colaboradores em qualquer posição hierárquica, preservando a comunicação e o relacionamento interpessoal construtivo.

7. Estimativa da demanda - quantidade de bens e serviços

7.1 O ICMBio possui um amplo parque computacional para atendimento aos usuários. Atualmente existem mais de 3000 usuários ativos na rede do ICMBio, de acordo com as licenças de suíte de escritório atribuídas aos servidores e colaboradores do Instituto.

7.2 O quantitativo foi estimado/definido com base no número de usuários licenciados com a suíte de aplicativos para escritório /produtividade Microsoft Office® (verificado no dia 10/08/2022 pelo portal de administração das licenças), tendo em vista que a rotatividade dos usuários ocorre com maior frequência do que a realização dos inventários. Além disso, verificou-se o quantitativo de máquinas virtuais no ambiente de produção.

7.2 Tendo em vista que há constantes alterações no quadro funcional do Instituto é salutar a criação de uma reserva técnica, que corresponda a 10% do quantitativo de licenças para computadores e notebooks, ou seja 311 equipamentos.

Item de Configuração	Quantitativo Estimado
Número de Usuários Ativos com licença Microsoft Office®	3.116
Reserva Técnica	311
Servidores virtuais ICMBio - Windows	20
Servidores virtuais ICMBio - Linux	208

7.3 Portanto, a estimativa total de equipamentos a serem protegidos e os serviços a serem contratados é o que consta na tabela abaixo

DESCRIÇÃO	UND.	QTDE
Serviço de proteção para computadores e notebooks	UNIDADE	3.427
Serviço de proteção para servidores de rede		228
Treinamento na solução contratada	PESSOAS	15

8. Levantamento de soluções

8.1 Abaixo foram relacionadas soluções aplicáveis ao objeto de estudo

1	Contratação de uma solução de proteção contra ameaças avançadas (Next Generation Antivírus - NGAV) baseada em agente com funcionalidade de EDR - (Endpoint Detection and Response).
2	Adesão à Ata de Registro de Preços
3	Outsourcing de Solução

9. Análise comparativa de soluções

9.1 Segue abaixo análise comparativa de soluções, conforme art.11, inciso II da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019:

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		
	Solução 3		X	
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1		X	
	Solução 2			X
	Solução 3			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X
	Solução 3			X

9.1 A análise comparativa de soluções, deve considerar, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação, observando, de acordo com o objeto em estudo:

1. necessidades similares em outros órgãos ou entidades da Administração Pública e as soluções adotadas;
2. a existência de software livre
3. as alternativas do mercado;

9.2 Um software da natureza do objeto deste estudo, ou uma solução corporativa de antivírus multiplataforma com gerenciamento centralizado, são arranjos de software de alta complexidade e com muitas funções incorporadas, não sendo desenvolvidos sob encomenda: são adquiridos por meio de licenças e necessitam de atualizações periódicas, sendo corriqueiro receberem mais de uma atualização ao dia. Assim, a busca por outro órgão público que possa ceder um software deste tipo, tendo desenvolvido solução semelhante não apresentou resultados positivos, uma vez que as licenças são exclusivas para os respectivos contratantes.

9.3 Ademais verificou-se que nos últimos meses, entre 2021 e 2022, foram feitas diversas aquisições, por meio de pregão eletrônico, pela Administração Publica, de objetos similares ao elencado aqui neste estudo. Podemos citar entidades como: INST. FED.DE EDUC., CIENCIA E TEC. DO MARANHÃO (Pregão 4/2022); DEPTO. NAC. DE INFRA-ESTRUTURA DE TRANSPORTES (Pregão 505/2021) ; FUNDAÇÃO UNIVERSIDADE DE BRASÍLIA - FUB (Pregão 208/2021); MJ-DPRF-DEPART.DE POL.RODOVIARIA FEDERAL/DF (Pregão 19/2021); MMA-IBAMA - DEFIN/DF (Pregão 4/2022), dentre outros.

9.4 Assim a procura seguiu para a busca de uma alternativa no portal Software Público Brasileiro, disponível em https://softwarepublico.gov.br. O referido site lista diversos softwares livres que atendem às necessidades de modernização da administração pública de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios e são compartilhados sem ônus, resultando na economia de recursos públicos e constituindo um recurso benéfico para a administração pública e para a sociedade. Em buscas realizadas no referido portal, não foram encontradas soluções livres que possam ser utilizadas para atendimento às necessidades do ICMBio no que tange a solução estudada. Dado o resultado negativo, as alternativas se voltam a soluções disponíveis de mercado.

9.5 As opções para solução corporativa de antivírus disponíveis no mercado se apresentam em grande quantidade e muitas versões. Para facilitar a escolha, existem entidades internacionais de consultoria que classificam os fabricantes conforme a sua desenvoltura no mercado. Uma dessas entidades, Gartner Group, relaciona os vários fabricantes de solução de antivirus tais como:

SentinelOne, CrowdStrike, VMware, Trend Micro; Microsoft; Check Point Software Technologies; WatchGuard; Broadcom (Symantec); Palo Alto Networks; Malwarebytes; Cybereason; Sophos; Cisco; Cynet; FireEye; Absolute; BlackBerry; Panda Security; McAfee; ESET; WithSecure; TEHTRIS; HarfangLab; Fortinet; Heimdal Security; Tanium; OpenText; 1E; Fidelis; Secureworks; IBM (ReaQta); Elastic; CyCraft; SecPod; Minerva Labs; Deep Instinct; Bitdefender; Sequretek; SlashNext; GoSecure; AhnLab ; ContraForce; Ziften; RSA; Digital Guardian.

9.6 As informações acima foram obtidas no endereço "https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions", de acesso público na internet em 10/08/2022.

9.7 Os fabricantes listados acima apenas exemplificam a variedades de fornecedores que existe no mercado e refletem a busca realizada no site da Gartner. Não pretende-se aqui fazer valoração entre um ou outro fabricante, cabendo aos licitantes interessados apresentarem propostas de acordo com o requisitos apresentados nestes estudo.

10. Registro de soluções consideradas inviáveis

10.1 A solução 2, (Adesão à Ata de Registro de Preços) é considerada inviável por não satisfazer plenamente as demandas do ICMBio, pois perde-se a autonomia de definição das especificações técnicas necessárias para atendimento das peculiaridades deste órgão, quantidades de licenças necessárias, colocando em risco a compatibilização com atual parque tecnológico já em utilização pela ICMBio, bem como os resultados finais pretendidos.

10.2 A solução 3 (Outsourcing de Solução) é considerada inviável por não satisfazer plenamente as demandas do ICMBio, pois não demonstra-se economicamente vantajosa para a administração, bem como não percebe-se maturidade suficiente no mercado para atender na íntegra o presente projeto e, ainda, vislumbra-se enormes dificuldades para identificar interessados na colocação de softwares locados por valores que justifiquem este tipo de contratação. Além do mais, poderia comprometer o sigilo de informações substanciais.

11. Análise comparativa de custos (TCO)

11.1 Tendo em vista que das 3 soluções apresentadas, somente a Solução 1 - Contratação de uma solução de proteção contra ameaças avançadas (Next Generation Antivírus - NGAV) baseada em agente com funcionalidade de EDR - (Endpoint Detection and Response) foi considerada viável para atendimento às necessidades do ICMBio e que conforme pesquisa realizada no Portal de Compras do Governo Federal (https://www.gov.br/compras/pt-br/acesso-a-informacao/consulta-detalhada) há vários órgãos /entidades que adquiriram serviço similar ao objeto deste estudo, esta Equipe de Planejamento da Contratação descreve abaixo resultado da referida pesquisa.

11.2 Conforme estabelece art. 5º da Instrução Normativa nº 73, de 05 de Agosto de 2020:

> *"A pesquisa de preços para fins de determinação do preço estimado em processo licitatório para a aquisição e contratação de serviços em geral será realizada mediante a utilização dos seguintes parâmetros, **empregados de forma combinada ou não**: (grifo nosso)*
>
> *(..)*
>
> *II - aquisições e contratações similares de outros entes públicos, firmadas no período de até 1 (um) ano anterior à data de divulgação do instrumento convocatório;*
>
> *(..)*
>
> *IV - pesquisa direta com fornecedores, mediante solicitação formal de cotação, desde que os orçamentos considerados estejam compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do instrumento convocatório.*
>
> *(..)*
>
> *§1º Deverão ser priorizados os parâmetros estabelecidos nos incisos I e II."*

11.3 Todos os dados da pesquisa de preço estão inseridas no ANEXO I - Pesquisa de Preço de Antivirus EDR. Abaixo segue quadro resumo:

VALOR MEDIANO DOS ITENS (Convertidos para 36 meses quando for o caso)	UNIDADE	VALOR UNITÁRIO
Serviço de proteção para computadores e notebooks	LICENÇA	150,00
Serviço de proteção para servidores de rede		153,83
Serviço de Treinamento	PESSOA	2.500,00

11.4 Conforme art. 6º da IN Nº 73, DE 5 DE AGOSTO DE 2020: *"Serão utilizados, como métodos para obtenção do preço estimado, a média, **a mediana** ou o menor dos valores obtidos na pesquisa de preços, desde que o cálculo incida sobre um conjunto de três ou mais preços, oriundos de um ou mais dos parâmetros de que trata o art. 5º, desconsiderados os valores inexequíveis, inconsistentes e os excessivamente elevados." (grifo nosso)*

11.5 Tendo em vista a estimativa da demanda apresentada no item 7 deste estudo, podemos estimar o valor da contratação:

ITEM	DESCRIÇÃO	UND.	QTDE	ANO 1	ANO 2	ANO 3	TOTAL
1	Serviço de proteção para computadores e notebooks	LICENÇA	3.427	171.350,00	171.350,00	171.350,00	514.050,00
2	Serviço de proteção para servidores de rede		228	11.691,08	11.691,08	11.691,08	35.073,24
3	Serviço de Treinamento na solução contratada	PESSOAS	15	37.500,00	0,00	0,00	37.500,00
TOTAL				**220.541,08**	**183.041,08**	**183.041,08**	**586.623,24**

12. Descrição da solução de TIC a ser contratada

12.1 A solução de tecnologia da informação indicada neste planejamento e que atende as necessidades do objeto deste estudo consiste nos seguintes elementos de fornecimento:

- Contratação de uma solução de proteção contra ameaças avançadas (Next Generation Antivírus - NGAV) baseada em agente com funcionalidade de EDR (“Endpoint Detection and Response”).

13. Estimativa de custo total da contratação

Valor (R$): 586.623,24

13.1 Conforme discriminado no item 11, a estimativa de custo total da contratação é de R$ **586.623,24** (quinhentos e oitenta e seis mil, seiscentos e vinte de três reais e vinte e quatro centavos), valor relativo aos 36 (trinta e seis) meses de garantia de disponibilização da solução.

14. Justificativa técnica da escolha da solução

14.1 A escolha pela solução de proteção contra ameaças avançadas (Next Generation Antivírus - NGAV) baseada em agente com funcionalidade de EDR (“Endpoint Detection and Response”) vai ao encontro das necessidades do ICMBio em garantir segurança de rede para os usuários prevenindo proativamente ataques cibernéticos que representam risco significativo de perca de dados do Instituto.

14.2 A solução de um antivirus com funcionalidade de EDR (“Endpoint Detection and Response”) permite que a equipe de Tecnologia da Informação do ICMBio por meio de um portal de gerenciamento central controle todos os endpoint, ou seja, todos os terminais, seja desktop, notebooks ou servidores de rede. Esse controle permite aplicação de regras de segurança, monitoramento de atividades suspeitas e trafego de dados.

14.3 Ainda, também pode restringir quais dispositivos podem ou não se conectar aos endpoints. Assim, pode-se impedir que um USB com uma carga útil de malware malicioso seja instalado em certas portas USB sem permissão.

14.4 Esta solução complementa os firewalls *next generation*, adquiridos e implantados em 2022 pelo ICMBio, tornando assim a rede de computadores mais robusta e mais segura aos seus usuários.

15. Justificativa econômica da escolha da solução

15.1 Conforme demonstrado no item 11, após realização de pesquisa de mercado, apurou-se o valor mediano de preços dos últimos pregões realizados e ainda com fornecedores de soluções para objetos similares e verificou-se que o valor mediano está em conformidade com os preços praticados no mercado.

15.2 Ademais, o prazo de vigência de 36 (trinta e seis) meses proporcionará maior vantajosidade econômica ao ICMBio, pois eliminará o custo administrativo da realização de novas licitações anuais, permitindo que a equipe de tecnologia da informação foque sua atuação na aplicação de métodos e procedimentos que agreguem valor tecnológico aos usuários dos serviços de tecnologia do Instituto.

16. Benefícios a serem alcançados com a contratação

16.1 Os resultados a serem alcançados são:

- Minimizar o máximo possível incidentes de seguranças que envolvam a rede do ICMBio;
- Permitir a atualização concorrente dos sistemas operacionais;
- Elevar o nível de proteção dos computadores desktops e notebooks do ICMBio;
- Elevar o nível de proteção dos servidores em operação no ICMBio.

17. Providências a serem Adotadas

17.1 Nenhuma providência adicional ou ajuste para a utilização da solução de proteção contratada será necessária.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

Em atendimento ao art. 11, Inciso V, § 1º e 3º, da Instrução Normativa/SGD/ME nº 01/2019, a equipe de elaboração entende que o estudo de soluções viáveis para esta demanda está de acordo com as necessidade do ICMBio, portanto, o presente Estudo Técnico Preliminar é justificadamente viável quanto aos requisitos de negócios, administrativos e técnicos a serem alcançados.

19. Responsáveis

ORDEM DE SERVIÇO Nº 253/2022/CGATI/DIPLAN/GABIN/ICMBIO, DE 04 DE AGOSTO DE 2022 (SEi 11730428)

RODRIGO DE SOUZA LOPES

Integrante Requisitante

ORDEM DE SERVIÇO Nº 253/2022/CGATI/DIPLAN/GABIN/ICMBIO, DE 04 DE AGOSTO DE 2022 (SEi 11730428)

MILENA ALVES PACHECO

Integrante Administrativo

ORDEM DE SERVIÇO Nº 253/2022/CGATI/DIPLAN/GABIN/ICMBIO, DE 04 DE AGOSTO DE 2022 (SEi 11730428)

RAFAEL FELIX DE SA SILVA

Integrante Técnico

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - Pesquisa de Preço de Antivirus EDR.pdf (465.14 KB)

Anexo I - Pesquisa de Preço de Antivirus EDR.pdf

MINISTÉRIO DO MEIO AMBIENTE
INSTITUTO CHICO MENDES DE CONSERVAÇÃO DA BIODIVERSIDADE
COORDENAÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

PESQUISA EM COMPRAS REALIZADAS PELA ADMINISTRAÇÃO PÚBLICA

UASG	ORGÃO/ENTIDADE	PREGÃO Nº	ITEM	OBJETO	VIGENCIA	QNT	VALOR ITEM	VALOR ITEM	VALOR ITEM	VALOR TOTAL	DATA DA HOMOLOGAÇÃO	FORNECEDOR	PRODUTO OFERECIDO
158128	INST.FED.DE EDUC., CIENCIA E TEC. DO MARANHÃO	4/2022	01	Solução corporativa de antivírus multiplataforma com gerenciamento centralizado, compreendendo fornecimento de: software de segurança tipo EndPoint para estações de trabalho e servidores, software para gerenciamento centralizado, serviço de implantação da solução adquirida, suporte técnico on-site, pelo período de 36 meses, e transferência de tecnologia e conhecimento via treinamento de capacitação	36 (trinta e seis) meses	4390	R$ 71,40	R$ -	R$ -	R$ 313.446,00	01/08/2022	40.584.096/0001-05 - CENTRO DE PESQUISAS EM INFORMATICA LTDA	Kaspersky Endpoint Security for Business SELECT
926349	CONSELHO REGIONAL DE FISIOTERAPIA E TERAPIA	8/2022	01	Pregão Eletrônico - O objeto da presente licitação é a escolha da proposta mais vantajosa para aquisição de Software Antivírus, na modalidade Endpoint Security, com console de gerenciamento único, para detecção e resposta a ameaças a servidores físicos e computadores que compõem a rede de informática do Conselho Regional de Fisioterapia e Terapia Ocupacional da 8 Região, conforme condições, quantidades e exigências estabelecidas no Edital e seus Anexos.	36 (trinta e seis) meses	60	R$ 139,41	R$ -	R$ -	R$ 8.364,60	09/06/2022	07.421.409/0001-20 - LINKSAN TECNOLOGIA LTDA	Bitdefender GravityZone Business Security Premium
393003	DEPTO. NAC. DE INFRA-ESTRUTURA DE TRANSPORTES	505/2021	01	Fornecimento de Solução Completa de Antivírus (Endpoint Protection + Endpoint Detection Response) para estações de trabalho (desktops/notebooks), incluindo o licenciamento, instalação, configuração, garantia e console de gerenciamento centralizado	36 (trinta e seis) meses	5200	R$ 91,80	R$ -	R$ -	R$ 477.360,00	30/03/2022	10.554.387/0001-81 - ISTI INFORMATICA & SERVICOS LTDA	Bitdefender GravityZone Ultra Security (NGAV + EDR)
			02	Fornecimento de Solução Completa de Antivírus (Endpoint Protection + Endpoint Detection Response) para estações de trabalho (desktops/notebooks), incluindo o licenciamento, instalação, configuração, garantia e console de gerenciamento centralizado	36 (trinta e seis) meses	400	R$ -	R$ 91,80		R$ 36.720,00			
			03	Treinameno	-	2	R$ -	R$ -	R$ 7.960,00	R$ 15.920,00		-	-
154040	FUNDAÇÃO UNIVERSIDADE DE BRASÍLIA - FUB	208/2021 (SRP)	01	Licenciamento de Direitos Permanentes de Uso de Software para Estação de Trabalho Solução de segurança (software corporativo de antivírus multiplataforma) para estações de trabalho e servidores no ambiente administrativo da REDUnB (LICENÇAS)	12 (doze) meses	4000	R$ 50,00	R$ -	R$ -	R$ 200.000,00	21/12/2021	20.040.746/0001-36 - M3 COMERCIO SOFTWARE EIRELI	Bitdefender Gravityzone Advanced Business Security
200109	MJ-DPRF-DEPART.DE POL.RODOVIARIA FEDERAL/DF	19/2021	01	Módulo de EPP (Plataforma de proteção de endpoint): solução implantada em dispositivos Endpoint para evitar ataques de malware baseados em arquivos, detectar atividades maliciosas e fornecer os recursos de investigação e correção necessários para responder a incidentes e alertas de segurança dinâmicos, incluindo software nas versões mais atuais, gerenciamento centralizado, licenciamento, suporte técnico e garantia pelo período contratual.	12 (doze) meses	8946	R$ 60,35	R$ -	R$ -	R$ 539.891,10	30/12/2021	21.547.011/0001-66 - ALLTECH - SOLUCOES EM TECNOLOGIA LTDA	Trend Micro Suite Smart Protection for Endpoints, Apex One Sandbox e Deep Security Non-Server e Apex One Endpoint Sensor
			02	Módulo de EDR (detecção e resposta a ameaças): Solução de monitoramento e resposta contínuos a ameaças avançadas de segurança cibernética, incluindo software, gerenciamento centralizado, licenciamento, suporte técnico e garantia pelo período contratual.	12 (doze) meses	8946	R$ -	R$ 53,54	R$ -	R$ 478.968,84			Trend Micro Apex One Endpoint Sensor
			05	Serviço de treinamento dos itens 1, 2 e 3 para 30 (trinta) colaboradores	-	30	R$ -	R$ -	R$ 1.666,67	R$ 50.000,00			-
193099	MMA-IBAMA - DEFIN/DF	4/2022	01	Aquisição/Contratação de solução de proteção para computadores desktops e notebooks com suporte e garantia por 12 meses.	12 (doze) meses	4900	R$ 33,72	R$ -	R$ -	R$ 165.228,00	21/03/2022	27.685.014/0001-42 - 5 INSTITUTO TECNOLOGICO - SOCIEDADE CIVIL DE PROFISSION	BlackBerry Protect + Optics – Devices – Gov - Support (5000 +)
			02	Aquisição/Contratação solução de proteção para servidores de rede com suporte e garantia por 12 meses.	12 (doze) meses	180	R$ -	R$ 133,33	R$ -	R$ 23.999,40			
383518	CONSELHO REGIONAL DE CONTABIL.DO EST. DO RJ	4/2022	01	Proteção antivírus para Computadores. F-Secure Business Suite Premium License, (válida por 36 meses), com implantação, suporte e treinamento	36 (trinta e seis) meses	205	R$ 195,11	R$ -	R$ -	R$ 39.997,55	01/04/2022	15.190.568/0001-90 - MESQUITA TECNOLOGIA DA INFORMACAO EIRELI	F-Secure Business Suite Premium License
			02	Proteção antivírus para Servidores. F-Secure Business Suite Premium License, (válida por 36 meses), com implantação, suporte e treinamento	36 (trinta e seis) meses	13	R$ -	R$ 153,83	R$ -	R$ 1.999,79			

MINISTÉRIO DO MEIO AMBIENTE
INSTITUTO CHICO MENDES DE CONSERVAÇÃO DA BIODIVERSIDADE
COORDENAÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

PESQUISA COM FORNECEDORES

EMPRESA	DESCRIÇÃO DO ITEM		QNT	VALOR ITEM	VALOR ITEM	VALOR ITEM	VALOR TOTAL	PRODUTO OFERECIDO
NETSAFE CORP	LICENCA PARA USO DE SOFTWARE - ATUALIZAÇÃO DE SUÍTE PARA PROTEÇÃO DE ESTAÇÕES DE TRABALHO E SERVIDORES COM DETECÇÃO E RESPOSTA A INCIDENTES (EDR), COMGARANTIA E SUPORTE TÉCNICO PELO PERÍODO DE 12 MESES	12 (doze) meses	3450	R$ 105,00	R$ -	R$ -	R$ 362.250,00	McAfee MVISION Endpoint Detection and Response (MVISION EDR)
	SERVICO DE TREINAMENTO NA AREA DE INFORMATICA - TREINAMENTO/ATUALIZAÇÃO TECNOLÓGICA NA SOLUÇÃO DE PROTEÇÃO DE ESTAÇÕES DE TRABALHO E SERVIDORES COM EDR (ANTIVÍRUS)	-	32	R$ -	R$ -	R$ 2.500,00	R$ 80.000,00	-
ISTI Informática e Serviços Ltda-ME	Serviço de proteção para servidores de rede, computadores e notebooks	36 (trinta e seis) meses	3655	R$ 184,37	R$ -	R$ -	R$ 673.872,35	BitDefender GravityZone Business Security Enterprise (NGAV + EDR)
	Serviço de capacitação na solução contratada	-	15			R$ 1.800,00		

VALOR MEDIANO DOS ITENS (Convertidos para 36 meses quando for o caso)	UNIDADE	150	153,83	R$ 2.500,00
Aquisição de licenças para estações de trabalho	LICENÇA	R$ 150,00		
Aquisição de licenças para servidores	LICENÇA		R$ 153,83	
Serviço de treinamento	PESSOA			R$ 2.500,00

Conforme art. 6º da IN Nº 73, DE 5 DE AGOSTO DE 2020: Serão utilizados, como métodos para obtenção do preço estimado, a média, a **mediana** ou o menor dos valores obtidos na pesquisa de preços, desde que o cálculo incida sobre um conjunto de três ou mais preços, oriundos de um ou mais dos parâmetros de que trata o art. 5º, desconsiderados os valores inexequíveis, inconsistentes e os excessivamente elevados.